Security architecture:

- Firewalls and tunnels
- Old-school vs new world
- OT/SCADA

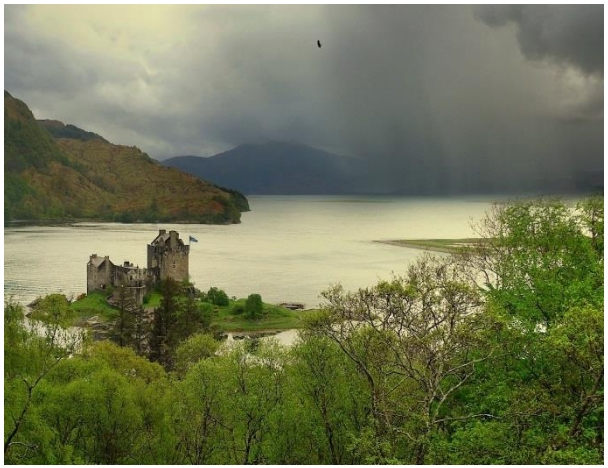
Hardware hacking

Carsten Jørgensen
Department of Computer Science

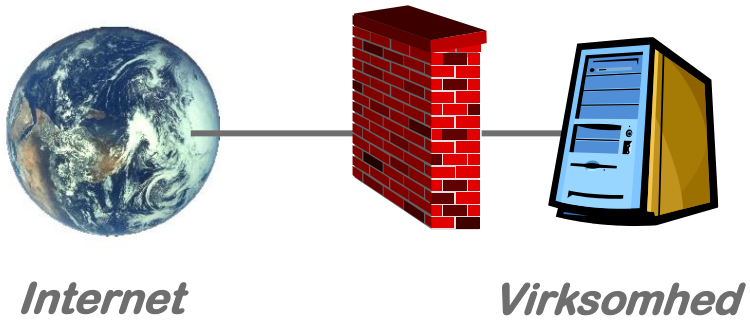
DIKU 3. November 2022

Security architecture, ports and firewalls

What is a firewall ?



Perimeter protection



Firewalls

Hardware or software designed to prevent unauthorized access through perimeter protection

Matches packets to policies, and applies different rules to different packets

Modern firewalls are hybrids and typically use multiple methods

Firewall types

Stateless: Do I like this packet?

Statefull: This packet is part of a flow. Do I like this flow?

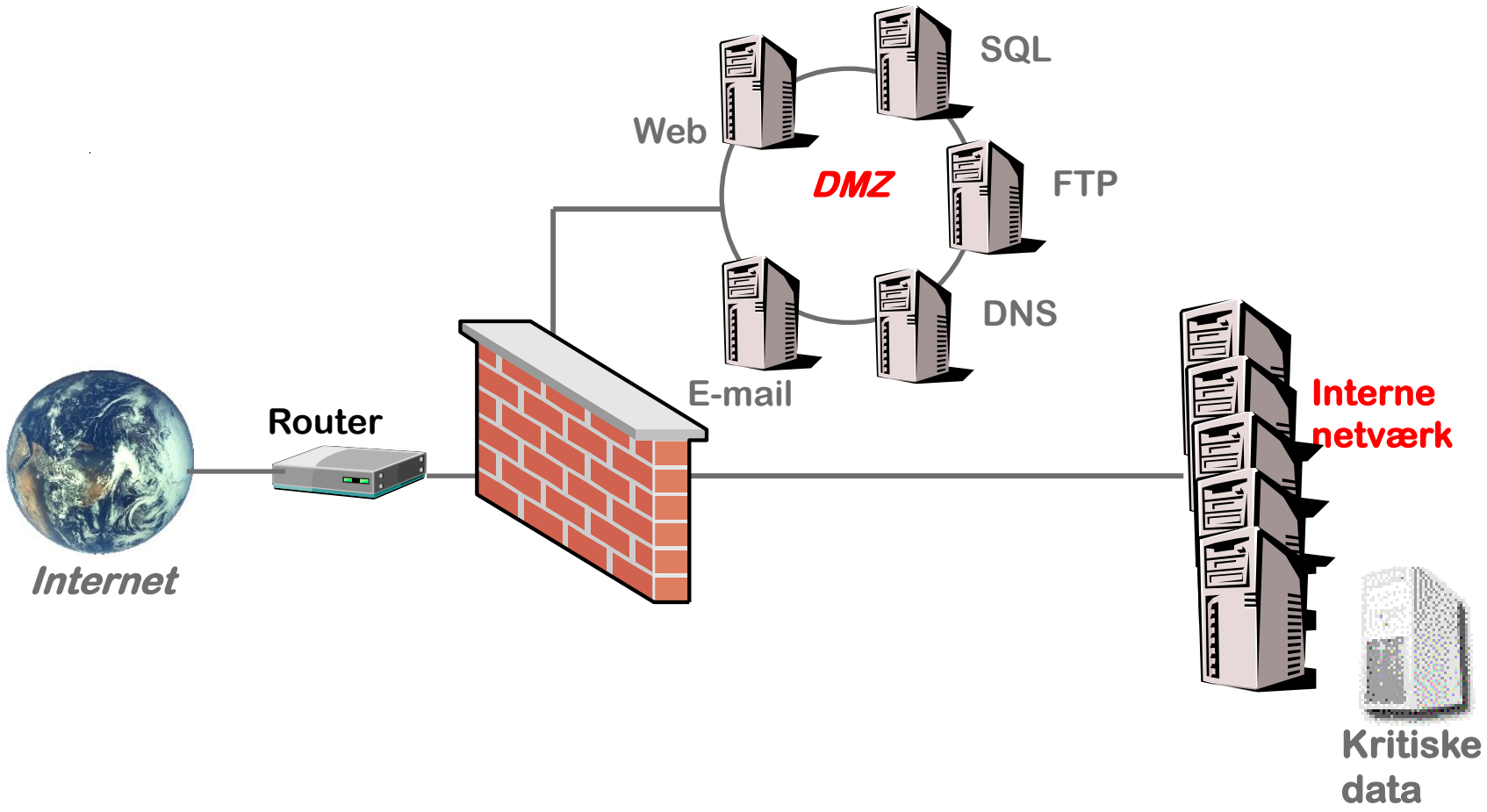
Firewall policies can be anything and can do anything

- Limit maximum bandwidth
- Increase minimum latency
- Alter content – add advertising into traffic

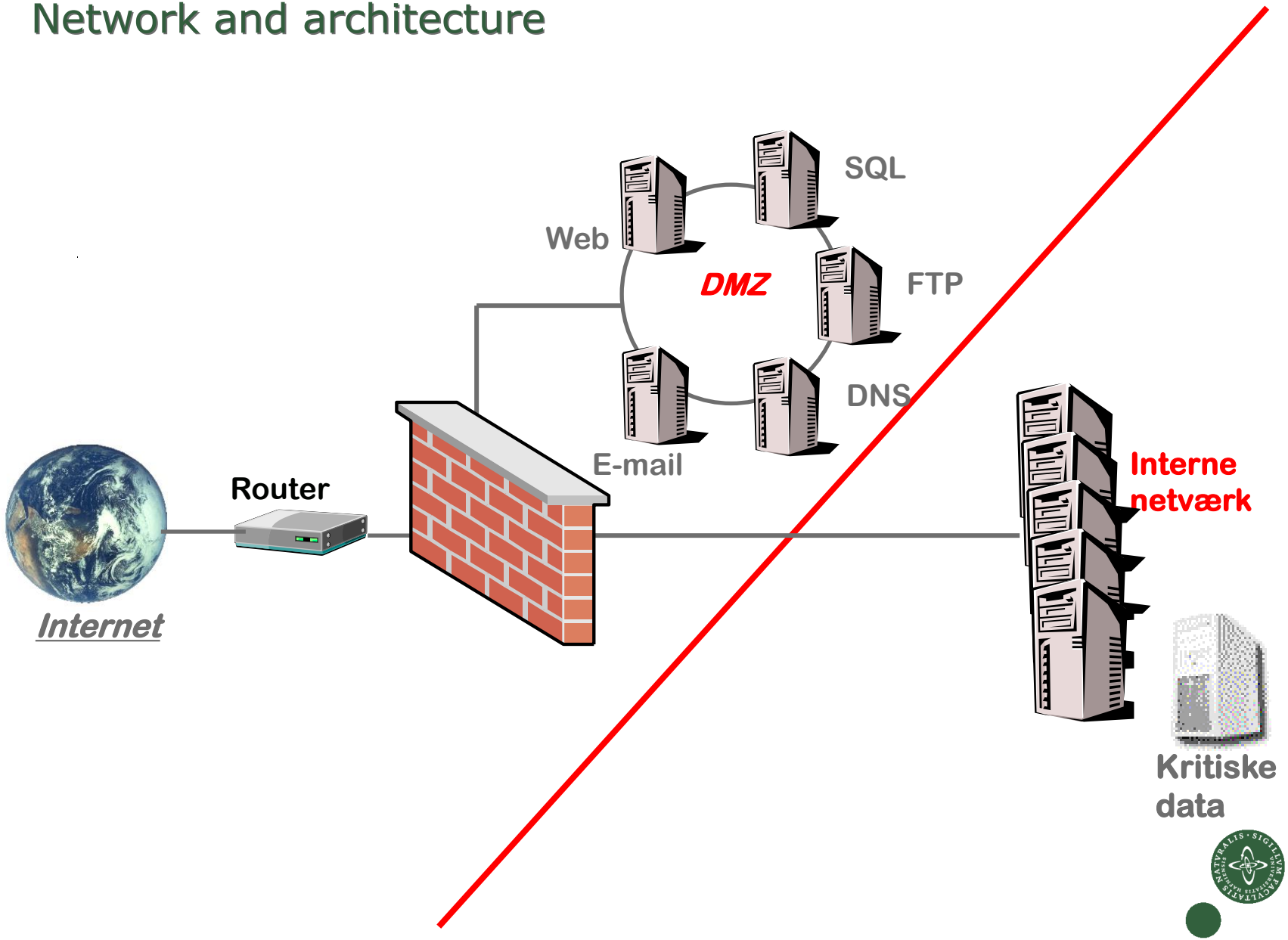
Firewall typer

- **Packet filter:** Looks at each packet entering or leaving the network and accepts or rejects it based on defined filter rules (addresses and port numbers). Packet filtering is fairly effective and transparent to users, but it is difficult to configure.
- **Stateful inspection / Circuit-level gateway:** Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can often flow between the hosts without further checking.
- **Application gateway:** Applies security mechanisms to specific applications, such as HTTP, FTP and Telnet servers. IP packets are not passed to internal hosts rather the application acts as an interpreter
  This is very effective, but can impose performance degradation.
- **WAF – Web Application Firewall**

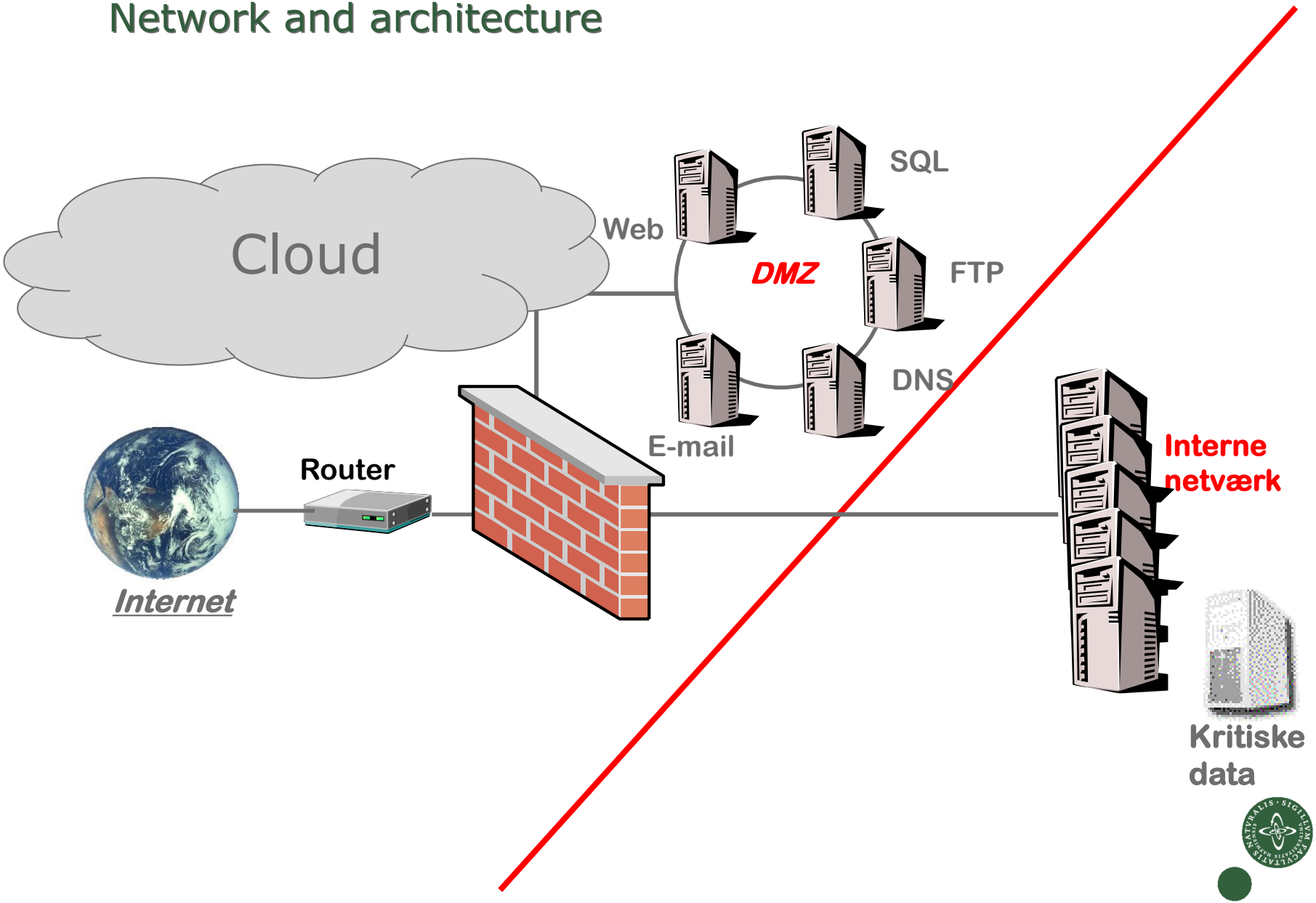
Network and architecture



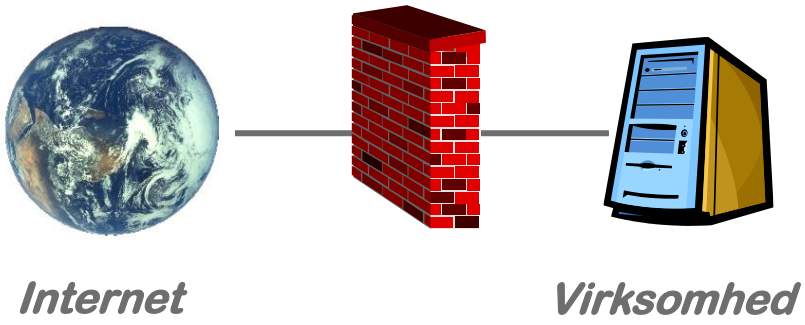
Network and architecture



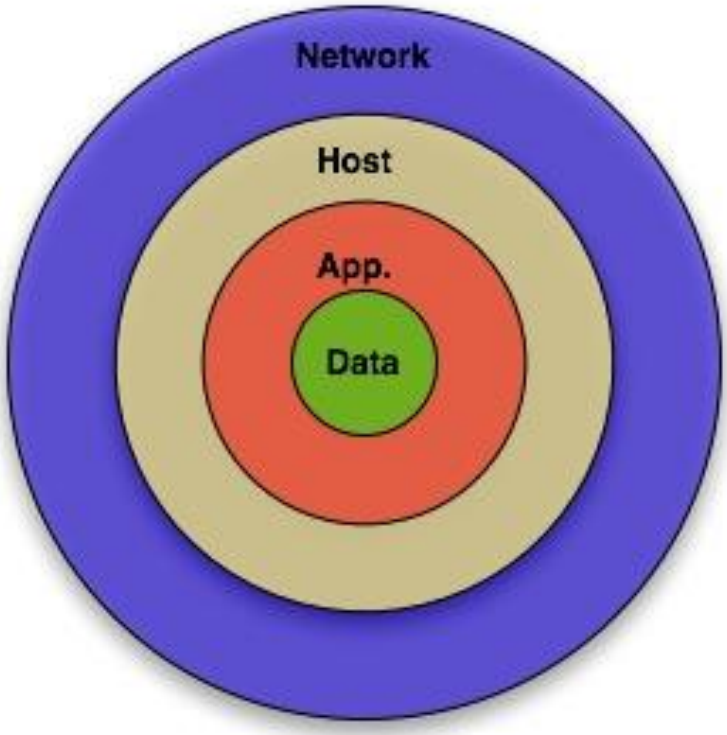
Network and architecture



Opening ports in the firewall

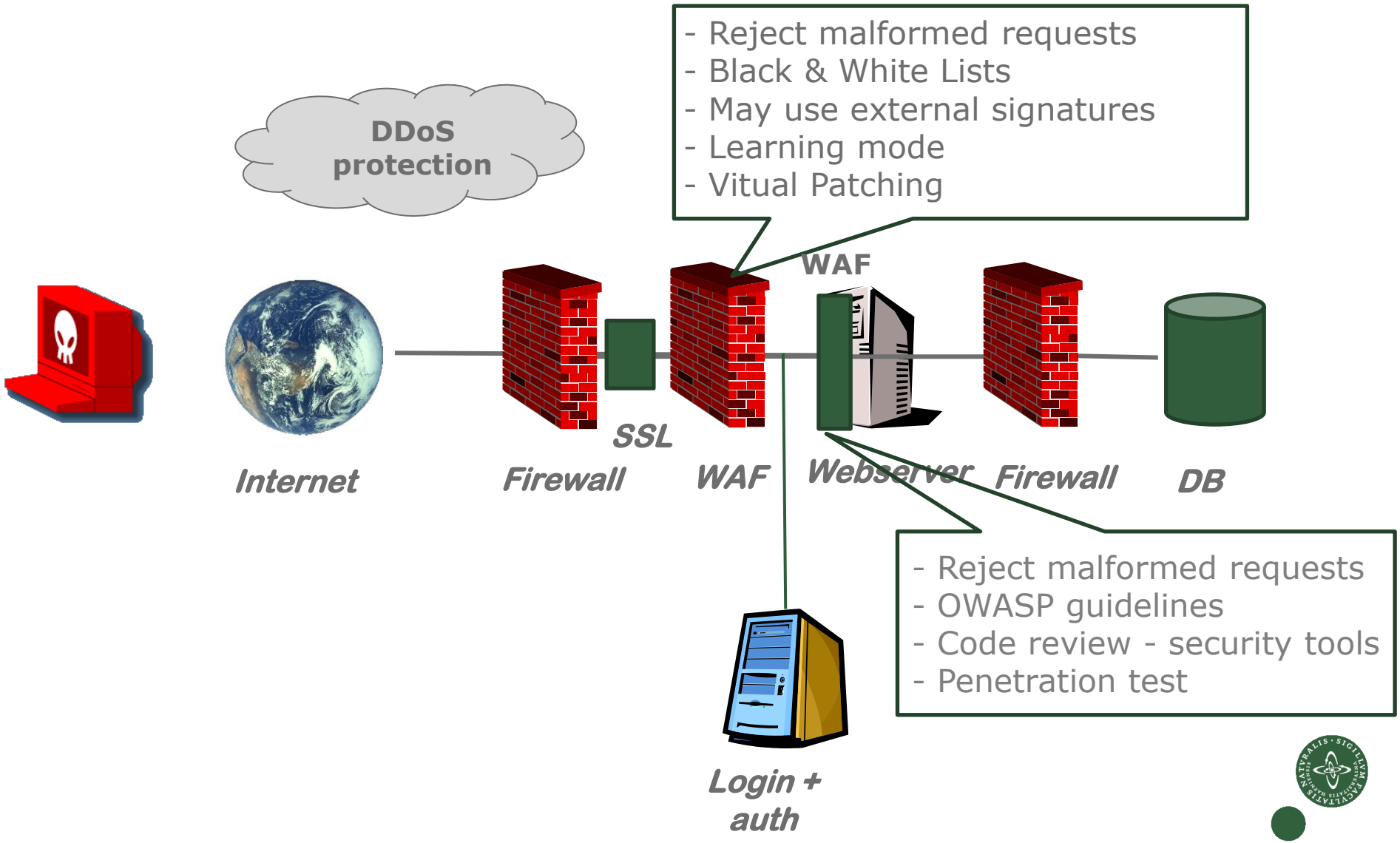


After opening?



Defense in Depth

Security architecture - Layers of security and the firewall



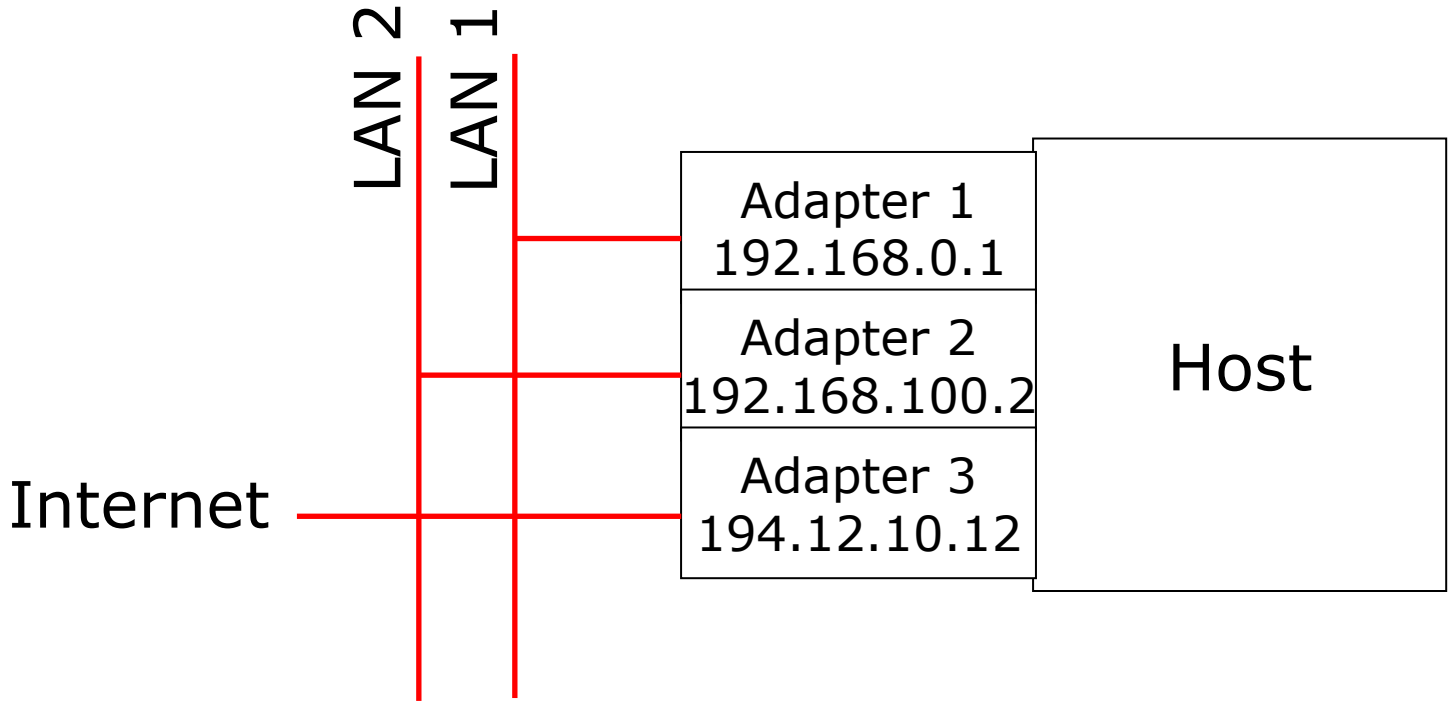
Which is "Best"?

Ports and firewalls

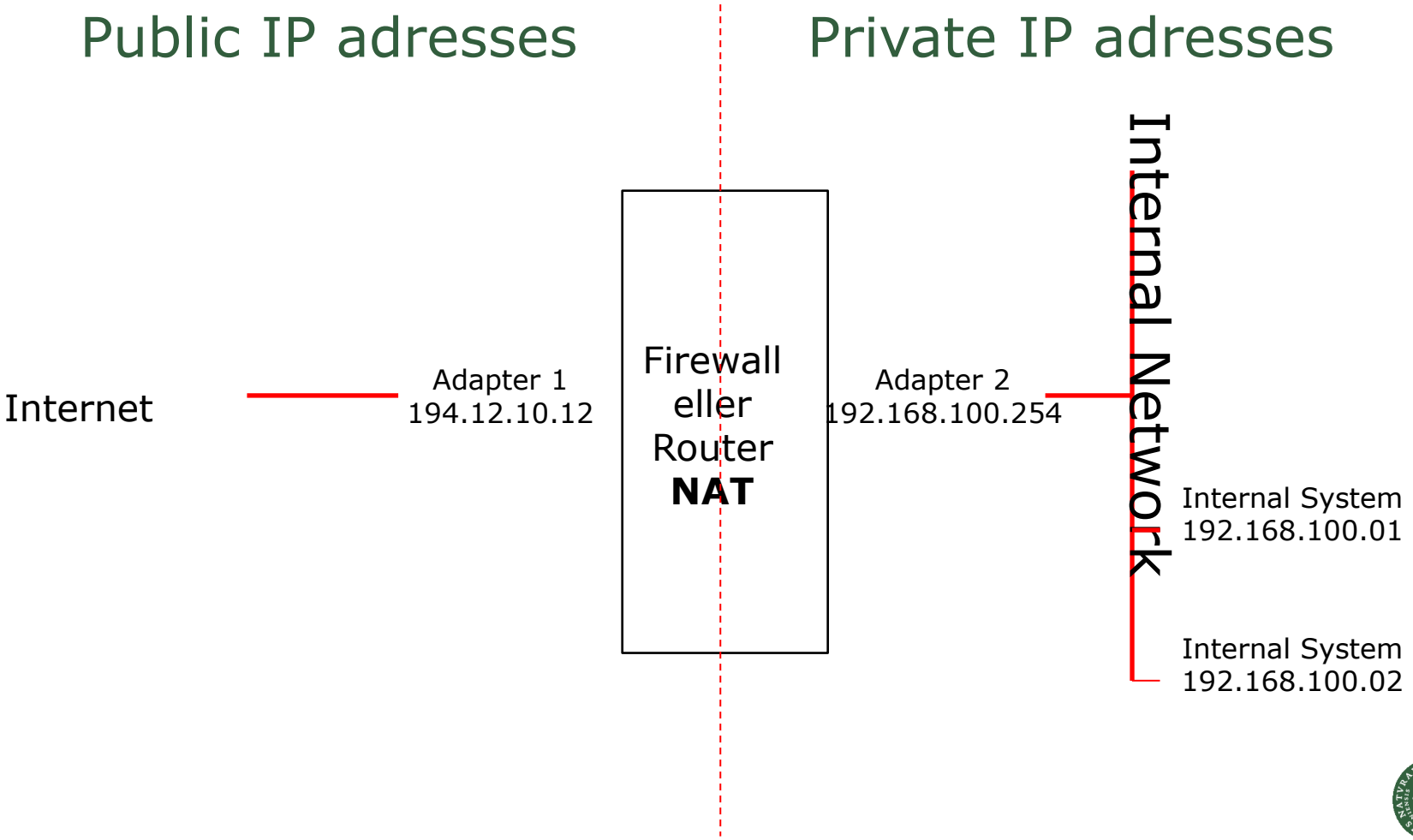
Firewalls – physically (or virtually)

IP addresses are associated with adapters, not CPUs

A single host can have many IP addresses



Network Address Translation (NAT)



Ports

To provide access to services over an IP-network applications are assigned a unique address – a port

The application binds to the port and starts when a connection-request is issued to the port

65.535 TCP and UDP ports

First 1024 ports are "*well known ports*", but services can be configured to run on all ports

1024 – 49151: Registred ports
49152 – 65535: dynamic and/or private ports

http://www.iana.org/assignments/port-numbers

IP + port: 192.168.10.1:80

A few well-known ports

Service	Port	Protocol
FTP	21	TCP
Telnet	23	TCP
Simple Mail Transfer Protocol (SMTP)	25	TCP
Domain Name	53	UDP
HTTP (web server)	80	TCP
POP3 (mail box)	110	TCP

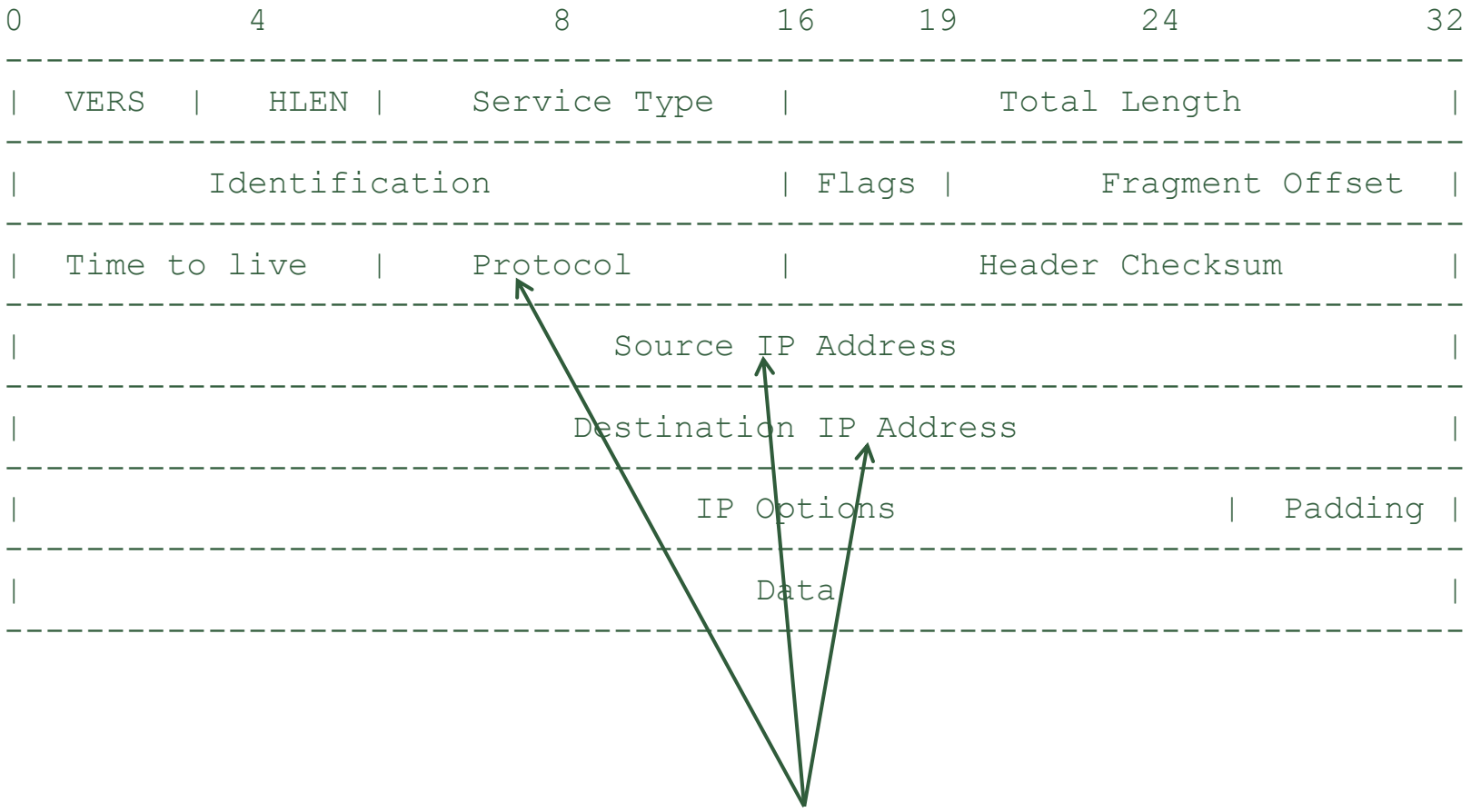
TCP/IP

- TCP - Transmission Control Protocol
- IP - Internet Protocol
- UDP - User Datagram Protocol (postcard)
- ICMP - Internet Control Message Protocol
- Many other protocols: IGMP, OSPF etc.

TCP - Transmission Control Protocol

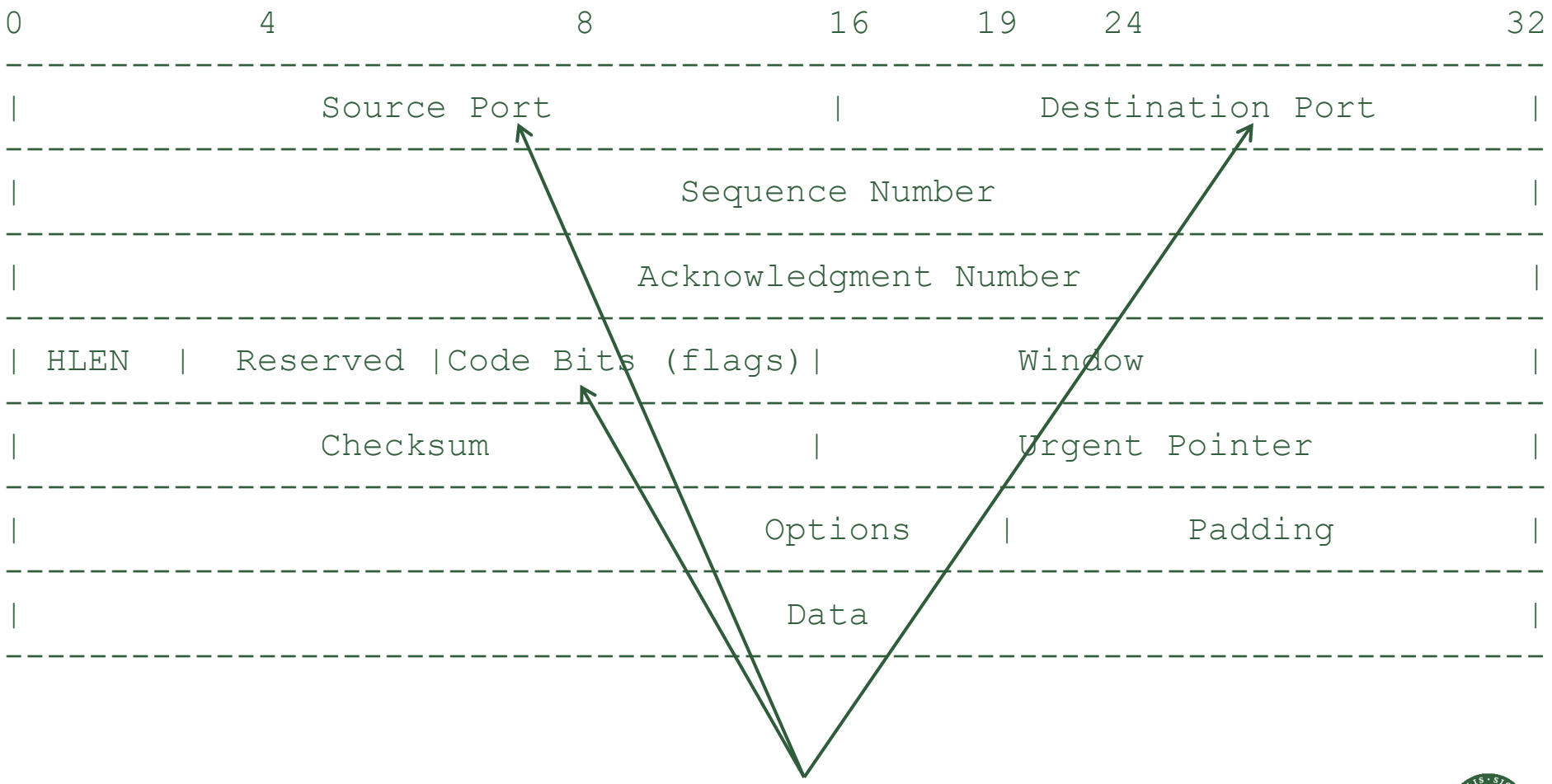
IP Header

Protocol	Source	Port	Destination	Port	Action
TCP	194.1.1.1	Any	180.2.2.2	80	Accept



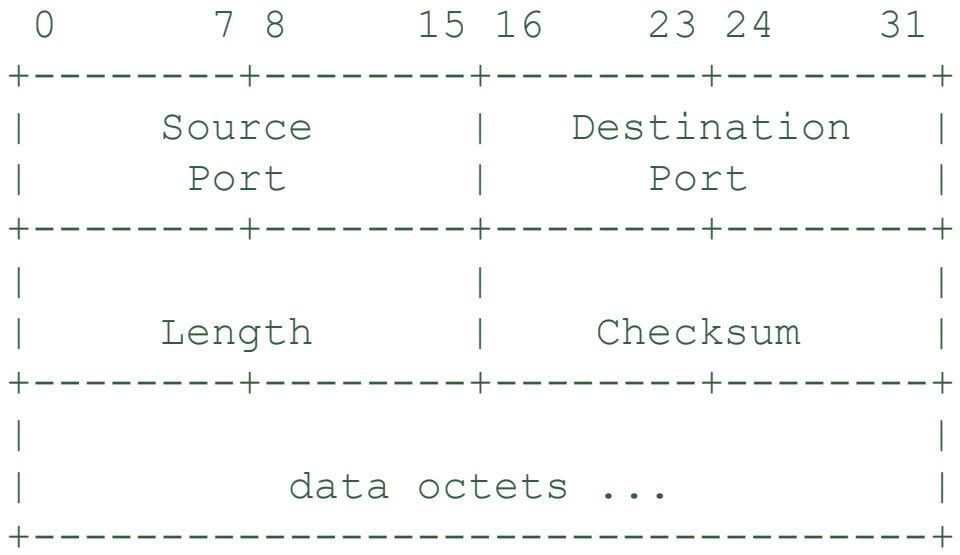
Typiske felter for filtrering

TCP Header



Typiske felter for filtrering

UDP header


0 7 8 15 16 23 24 31
Source Port
Destination Port
Length
Checksum
data octets ...

Firewall – basic terminology

- Firewall policy
- Firewall rules

Protocol	Source	Port	Destination	Port	Action
TCP	194.1.1.1	Any	180.2.2.2	80	Accept
TCP	Any		Any		Deny

Default-deny policy
Outbound filter

Block unwanted traffic, direct incoming traffic to internal nodes
Hide vulnerable nodes from external threats, log traffic to and from the network

Firewall rules

Rule #	Source	Destination	Protocol	Destination port	Action
1	External	Webserver	TCP	80	Allow
2	Hacker	Internal	Any	Any	Drop
3	210.1.2.3	10.0.0.7	TCP	37337	Allow

Word variations:
deny/forbid/disallow/drop/block/refuse

Packet-Filtering Examples - SMTP

Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Example Stateful Firewall - Connection State Table

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

Firewall Rulesets - Comments

Rule #	Action	Path	Source addr	Source port	Destination addr	Destination port	Protocol	Extra field	Comments
1	NO	in	us	*	*	*	*		ingress and egress
2	NO	out	them	*	*	*	*		filtering (Sect. 11.3)
3	NO	in	listed	*	*	*	*		block bad servers
4	OK	in	them	high	GW	25	TCP		inbound mail...
5	OK	out	GW	25	them	high	TCP	ACK	...our responses out
6	OK	out	GW	high	them	25	TCP		SMTP mail out...
7	OK	in	them	25	GW	high	TCP	ACK	...inbound response
8	OK	out	us	high	them	80	TCP		HTTP request out...

IPtables

https://www.frozentux.net/iptables-tutorial/iptables-tutorial.html#HOWARULEISBUILT

iptables -F INPUT *(flush)*

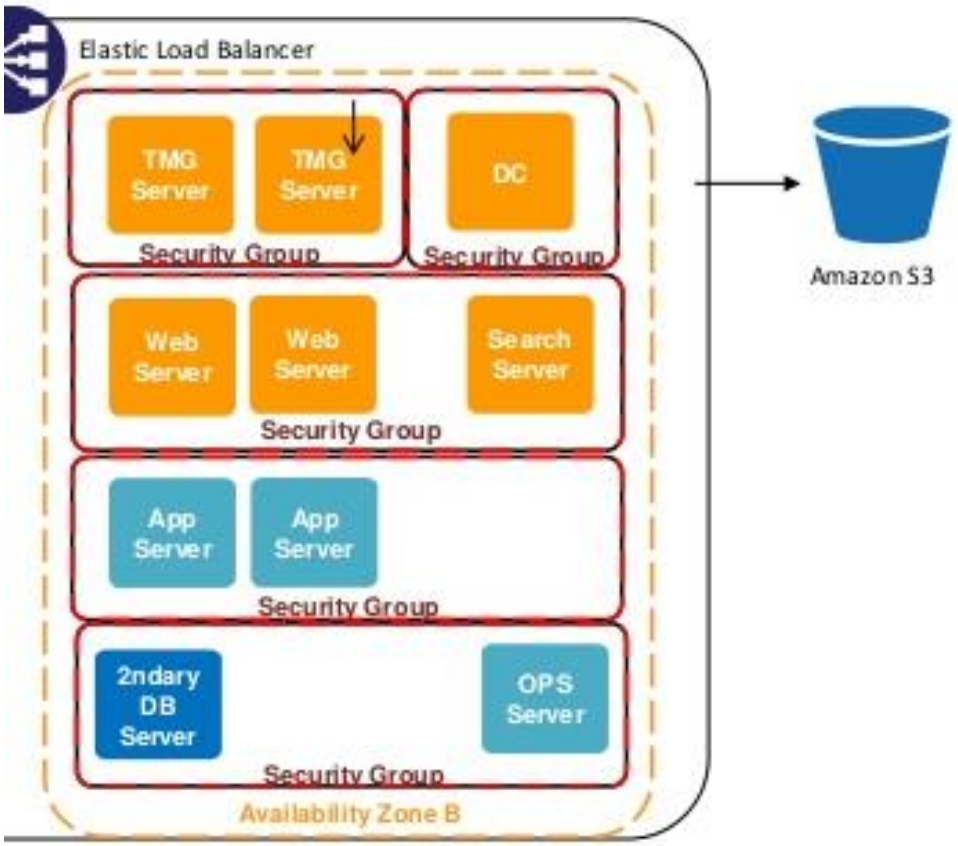
iptables -A INPUT -i eth0 -j DROP *(append)*

Firewalls and Security Groups

Security Groups

A *Security Group* is like a 'basic stateless firewall'

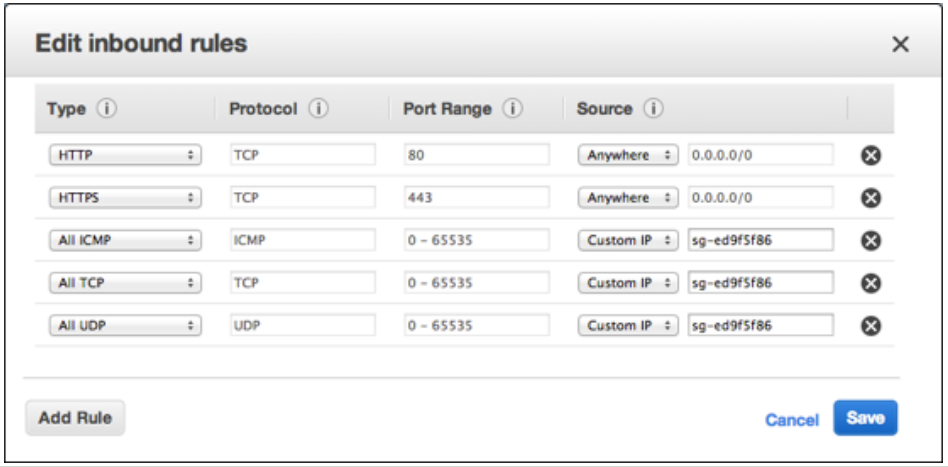
A Security Group is a container for security group rules. Works as firewalls – isolating traffic to VMs, controlling traffic to and from ports and instances



Security Groups – Cloud computing

- One or more Security Groups can be assigned to an instance

- Security group rules control the inbound traffic allowed to reach the instances associated with the security group.
  All other inbound traffic is discarded, and all outbound traffic is allowed by default.



Security Groups

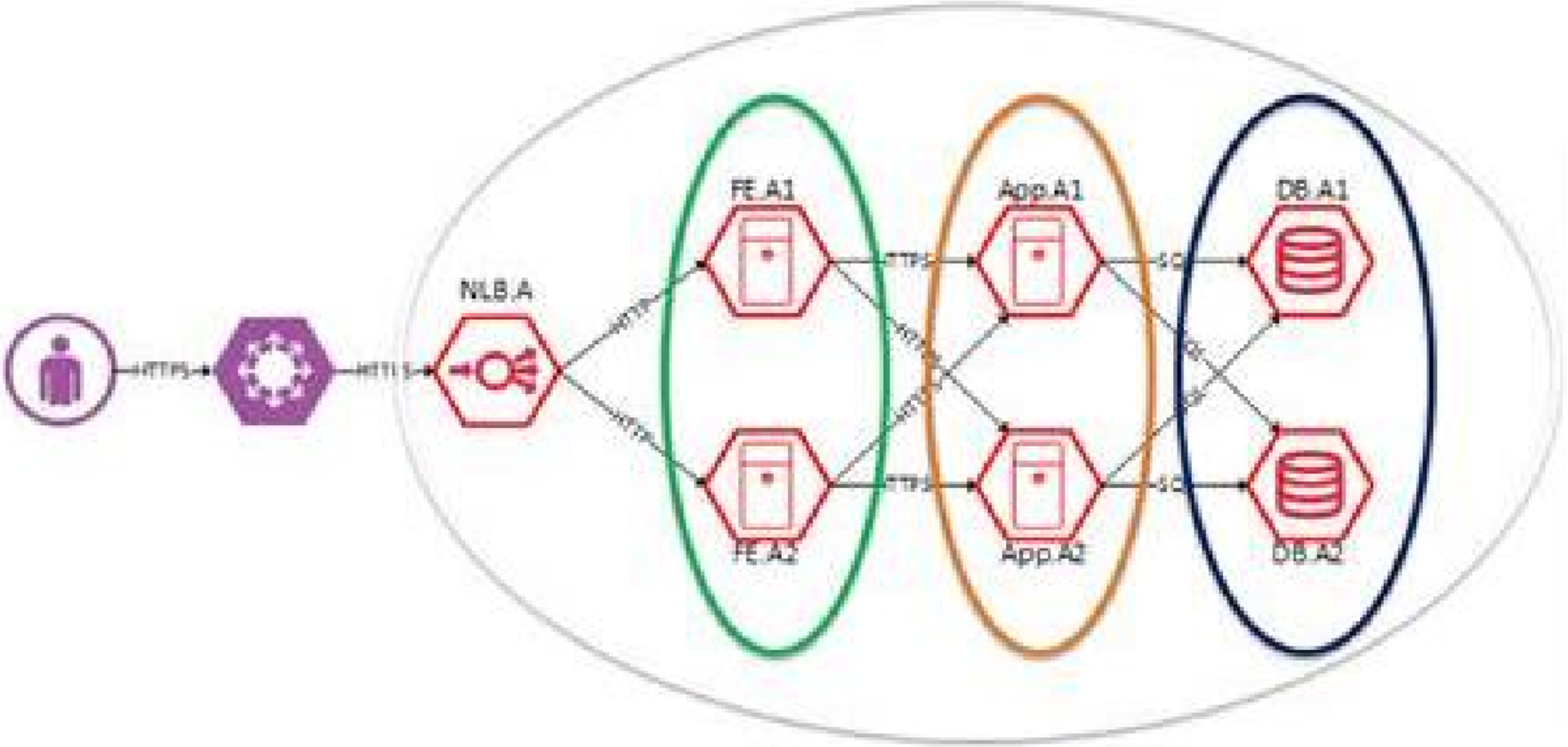
Instances in a Security Group cannot communicate with other instances unless specifically allowed.

"Small cheap firewalls" in front of every single server/system.

As default are each instance firewalled from other instances – level of segmentation that is almost impossible outside cloud.

SDN – "Software Defined Networking"

Microsegmenting – no trust (SDN)



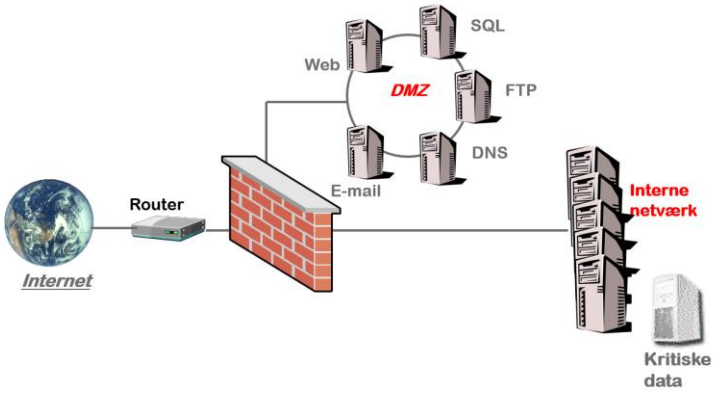
Security Groups

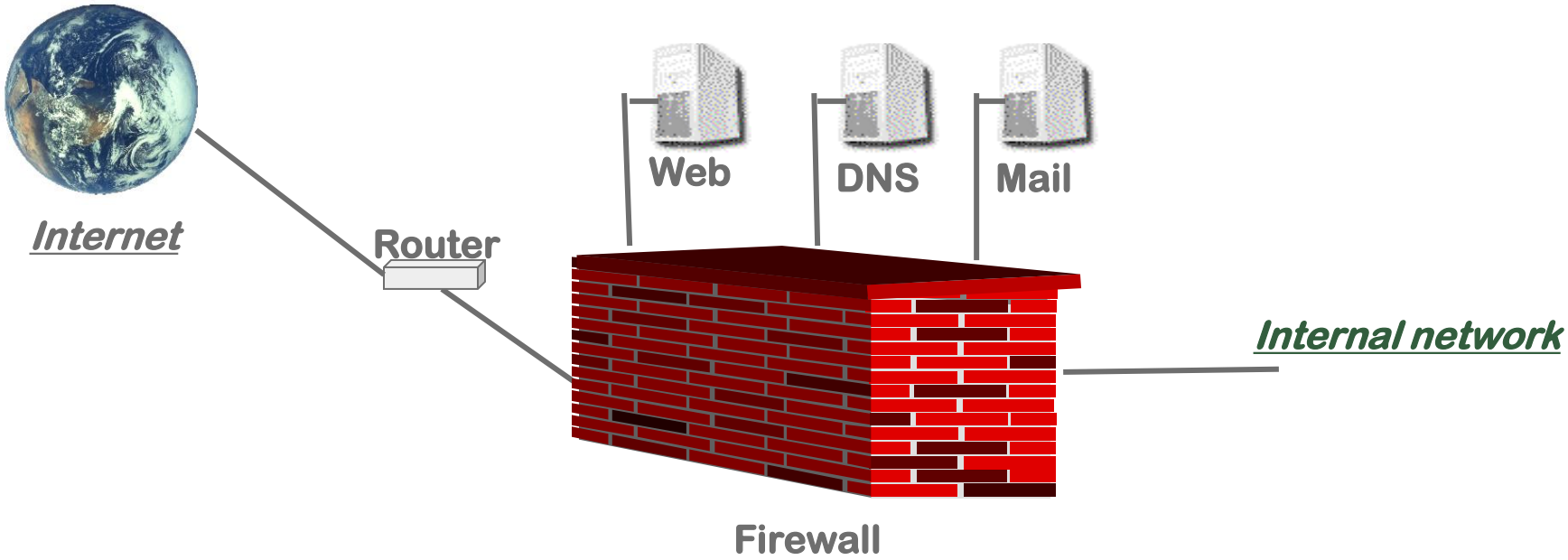
If a solutions has a number of web-, application and database servers each group is placed in a Security Group that only allows communication with layers directly above and below.

Security Groups should not allow any form of internet access outside the webserver group). Administrative access should be limited to known IP-addresses such as jump servers or own internal IP-addresses

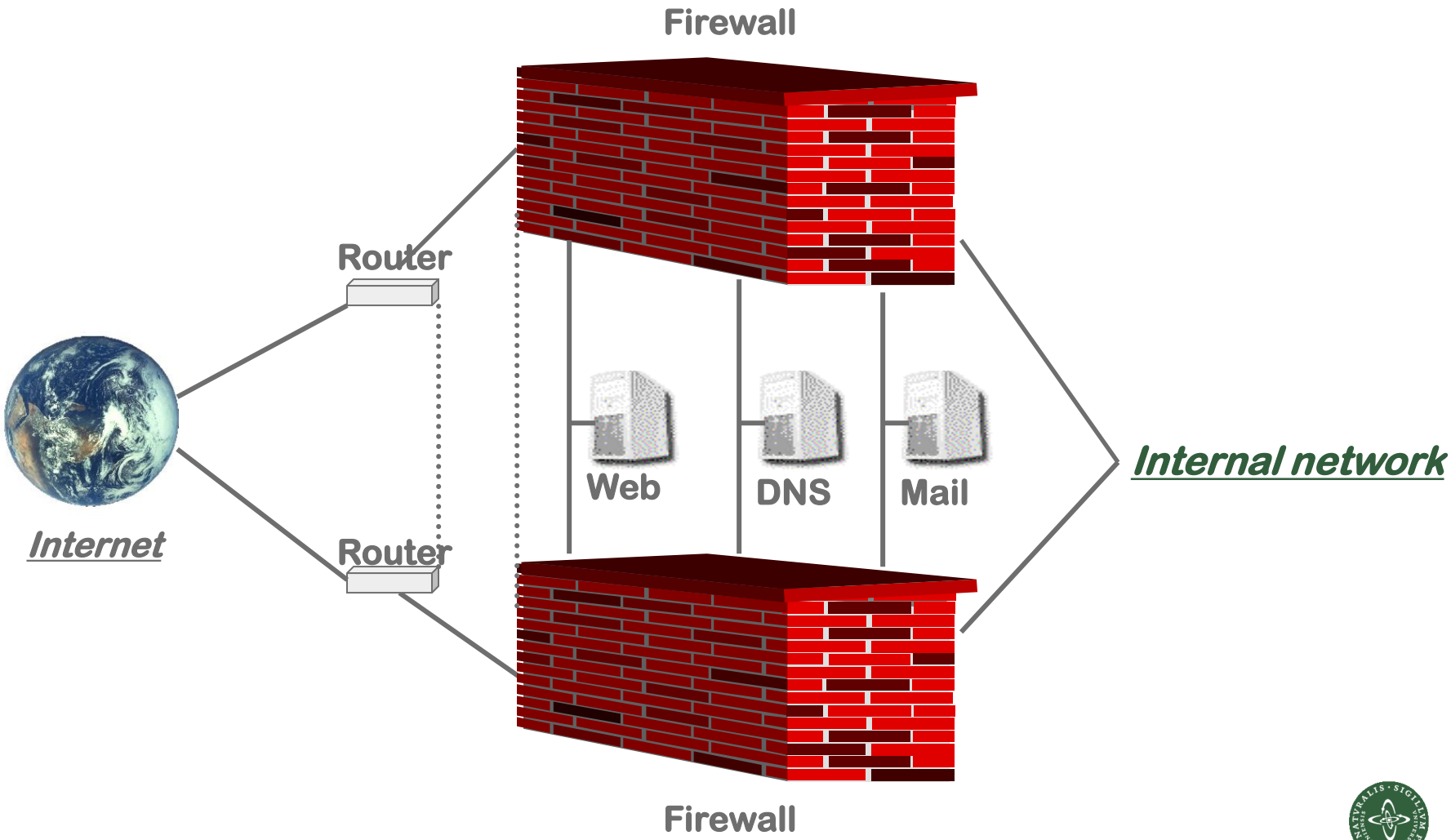
Security architecture: classic security measures

Multiple DMZ

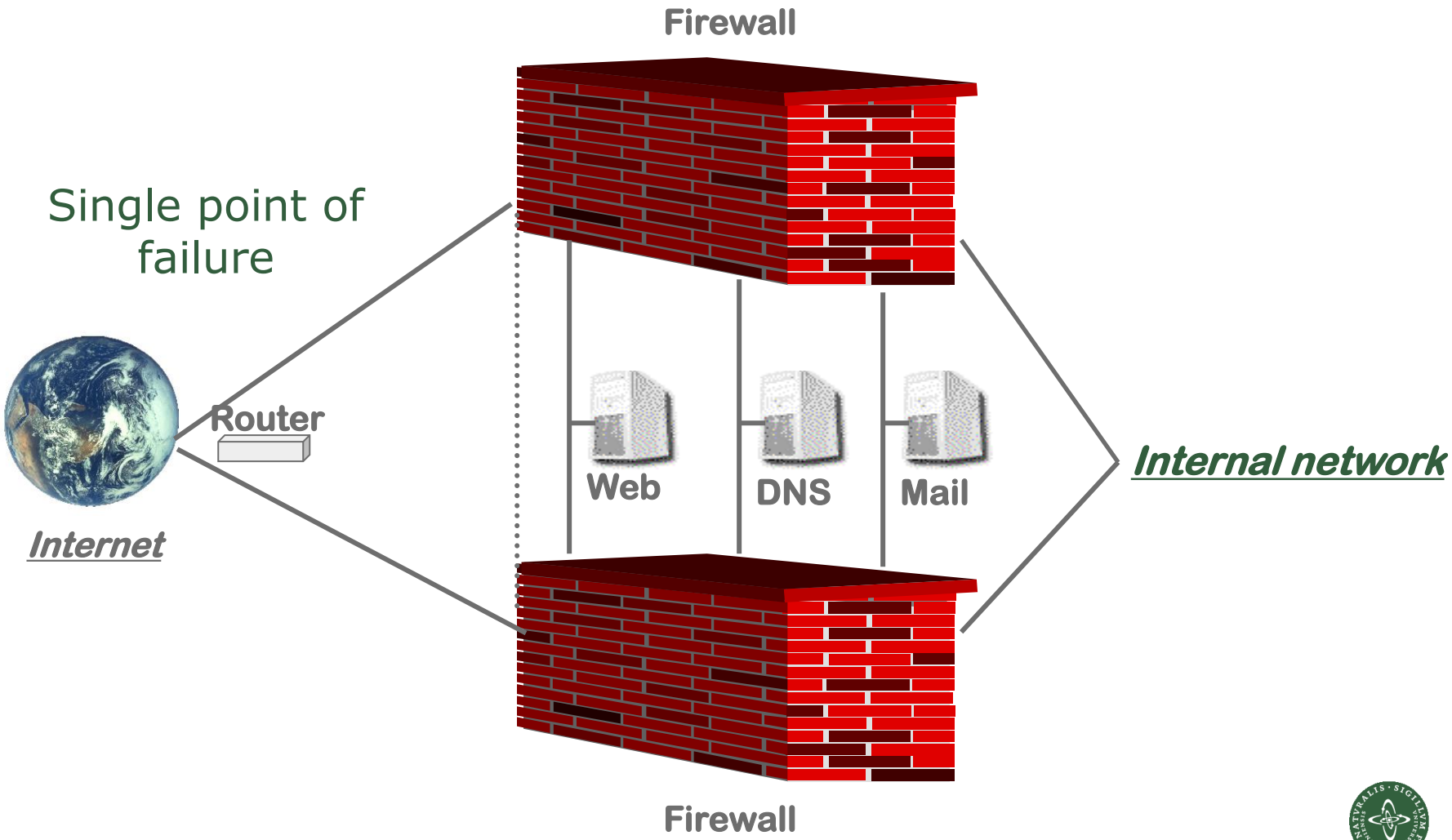




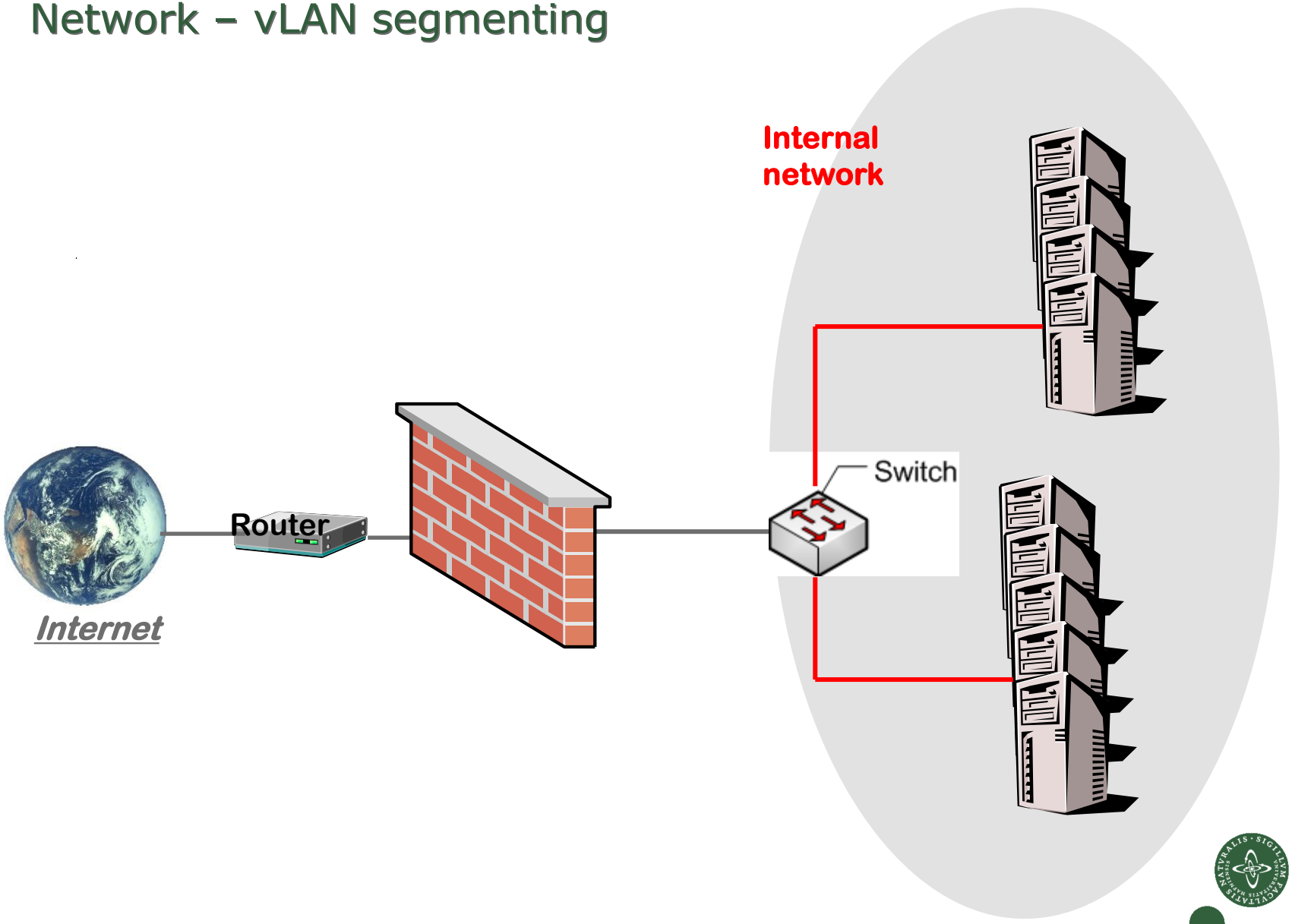
Multiple firewalls



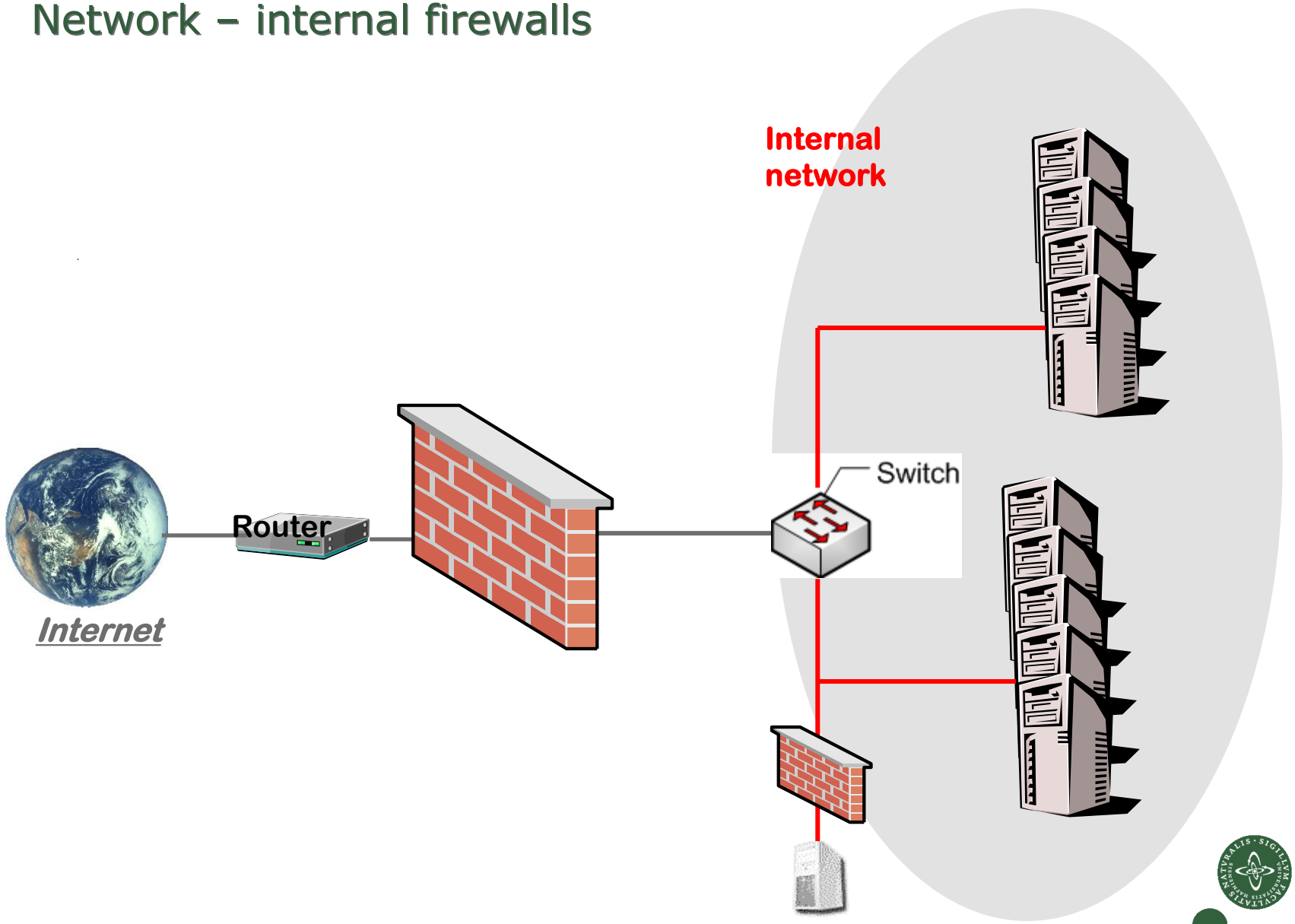
Multiple firewalls



Network – vLAN segmenting



Network – internal firewalls



Intrusion Detection Systems (IDS)
Intrusion Protection Systems (IPS)

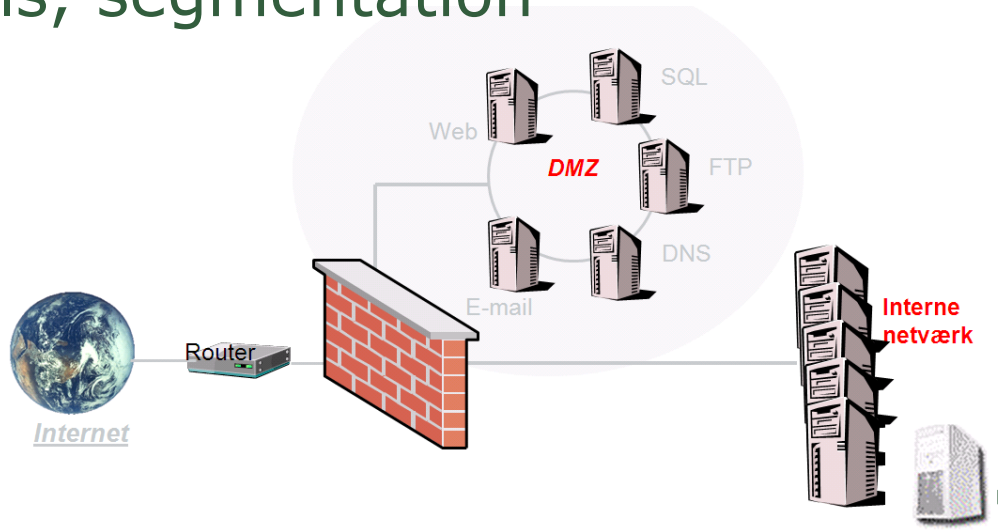
Intrusion Prevention Systems (IPS)

- Also known as Intrusion Detection and Prevention System (IDPS)
- Is an extension of an IDS that includes the capability to attempt to block or prevent detected malicious activity
- Can be host-based, network-based, or distributed/hybrid
- Can use anomaly detection to identify behavior that is not that of legitimate users, or signature/heuristic detection to identify known malicious behavior can block traffic as a firewall does, but makes use of the types of algorithms developed for IDSs to determine when to do so

Encrypted traffic?

More examples of security measures

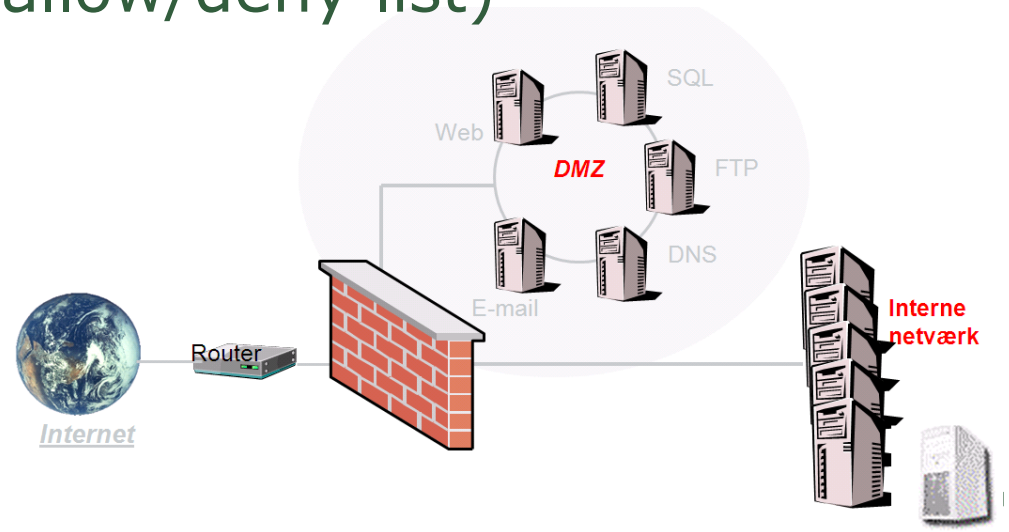
- IDS/IPS
- Scanning for virus and webtraffic
- Central loghost
- SIEM (Security Information and Event Mangement – log collection)
- Many DMZ's
- VLAN, internal firewalls, segmentation
- DDoS protection
- DNS security
- …



Prevent – Detect - Respond

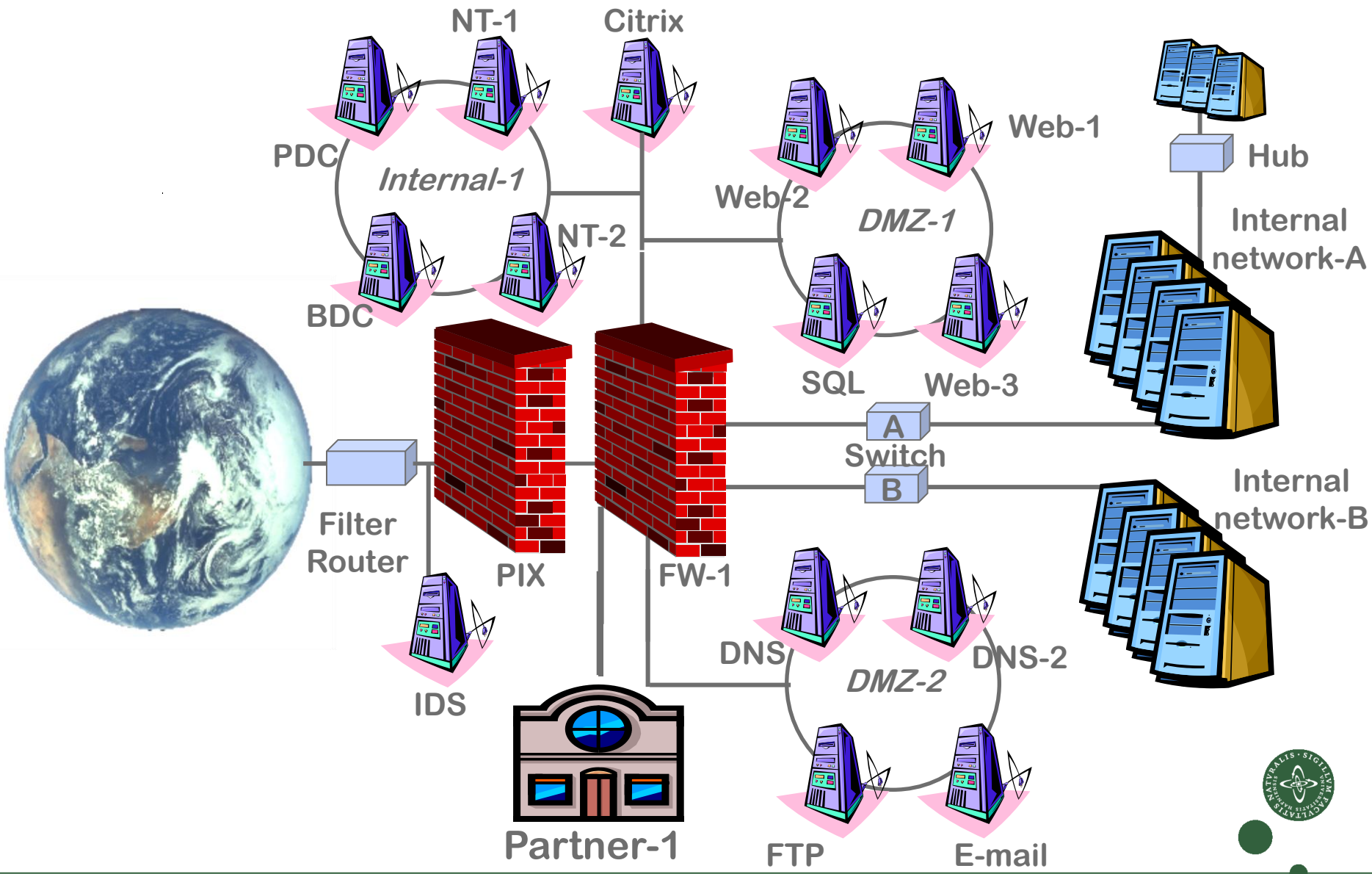
More examples of security measures

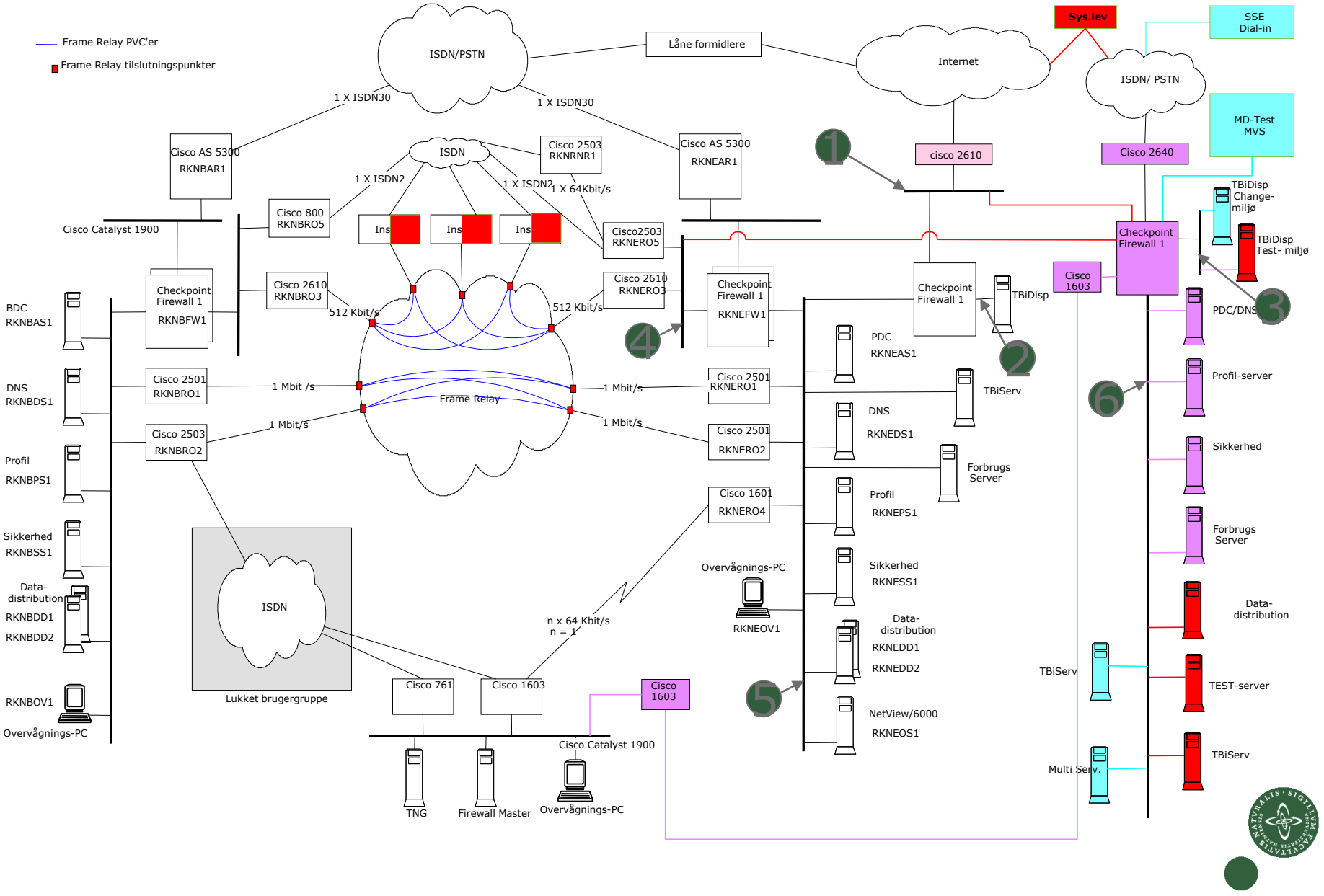
- Patching/updating
- Configuration management
- Filtering outgoing traffic
- Minimizing number of services (hardening)
- Whitelist/blacklist (allow/deny list)
- …



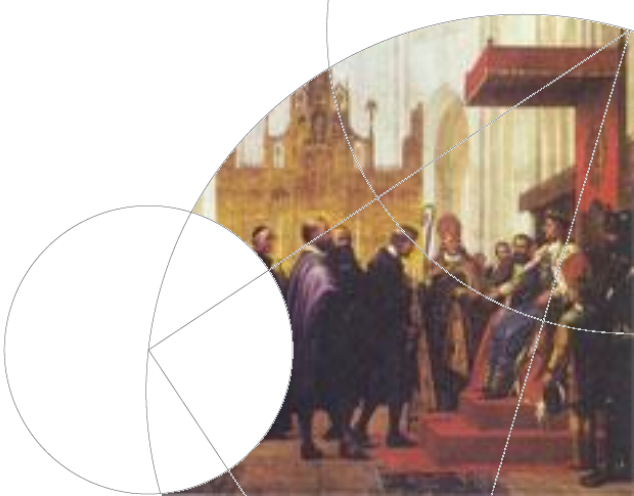
Prevent – Detect - Respond

Large network (example)

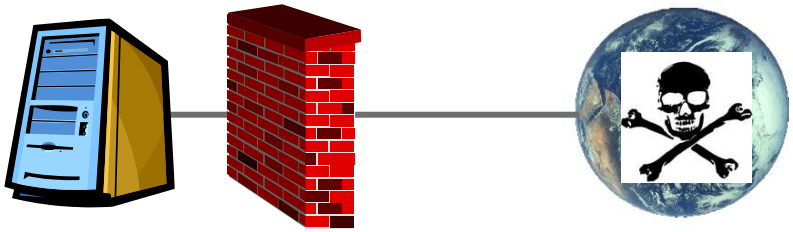



Frame Relay PVC'er
Frame Relay tilslutningspunkter
ISDN/PSTN
Låne formidlere
Internet
Sys.lev
SSE
Dial-in
ISDN/ PSTN
MD-Test
MVS
1 X ISDN30
1 X ISDN30
Cisco AS 5300
RKNBAR1
ISDN
Cisco 2503
RKNRNR1
Cisco AS 5300
RKNEAR1
cisco 2610
Cisco 2640
1 X ISDN2
1 X ISDN2
1 X 64Kbit/s
TBiDisp
Change-
miljø
TBiDisp
Test- miljø
Cisco Catalyst 1900
Cisco 800
RKNBRO5
Ins
Ins
Ins
Cisco2503
RKNERO5
Checkpoint
Firewall 1
Cisco
1603
BDC
RKNBAS1
Checkpoint
Firewall 1
RKNBFW1
Cisco 2610
RKNBRO3
512 Kbit/s
512 Kbit/s
Cisco 2610
RKNERO3
Checkpoint
Firewall 1
RKNEFW1
Checkpoint
Firewall 1
TBiDisp
PDC/DNS
PDC
RKNEAS1
DNS
RKNBDS1
Cisco 2501
RKNBRO1
1 Mbit /s
Frame Relay
1 Mbit/s
Cisco 2501
RKNERO1
TBiServ
Profil-server
DNS
RKNEDS1
Profil
RKNBPS1
Cisco 2503
RKNBRO2
1 Mbit/s
1 Mbit/s
Cisco 2501
RKNERO2
Forbrugs
Server
Sikkerhed
Profil
RKNEPS1
Sikkerhed
RKNBSS1
Cisco 1601
RKNERO4
Forbrugs
Server
Overvågnings-PC
Sikkerhed
RKNESS1
Data-
distribution
RKNBDD1
RKNBDD2
ISDN
Data-
distribution
RKNEDD1
RKNEDD2
Data-
distribution
n x 64 Kbit/s
n = 1
RKNEOV1
TBiServ
TEST-server
RKNBOV1
Overvågnings-PC
Lukket brugergruppe
Cisco 761
Cisco 1603
Cisco
1603
NetView/6000
RKNEOS1
Cisco Catalyst 1900
Multi Serv.
TBiServ
TNG
Firewall Master
Overvågnings-PC

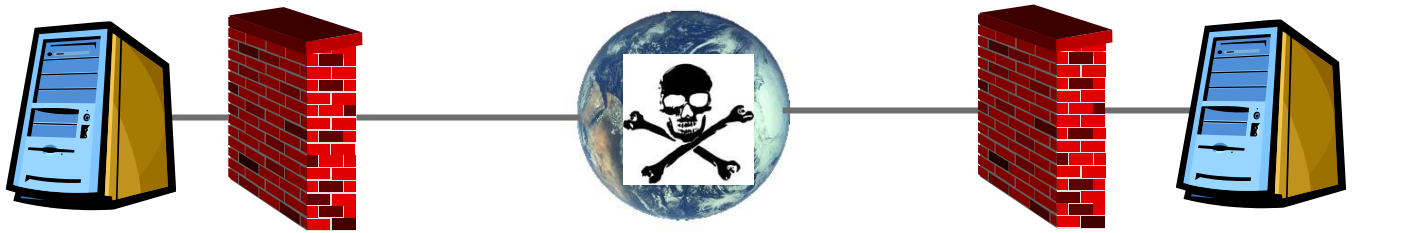
Tunnels



The need for tunnels



"I'm ok – but we can't trust the network"



"I'm ok, and you're ok – but we can't trust the network"

The need for tunnels

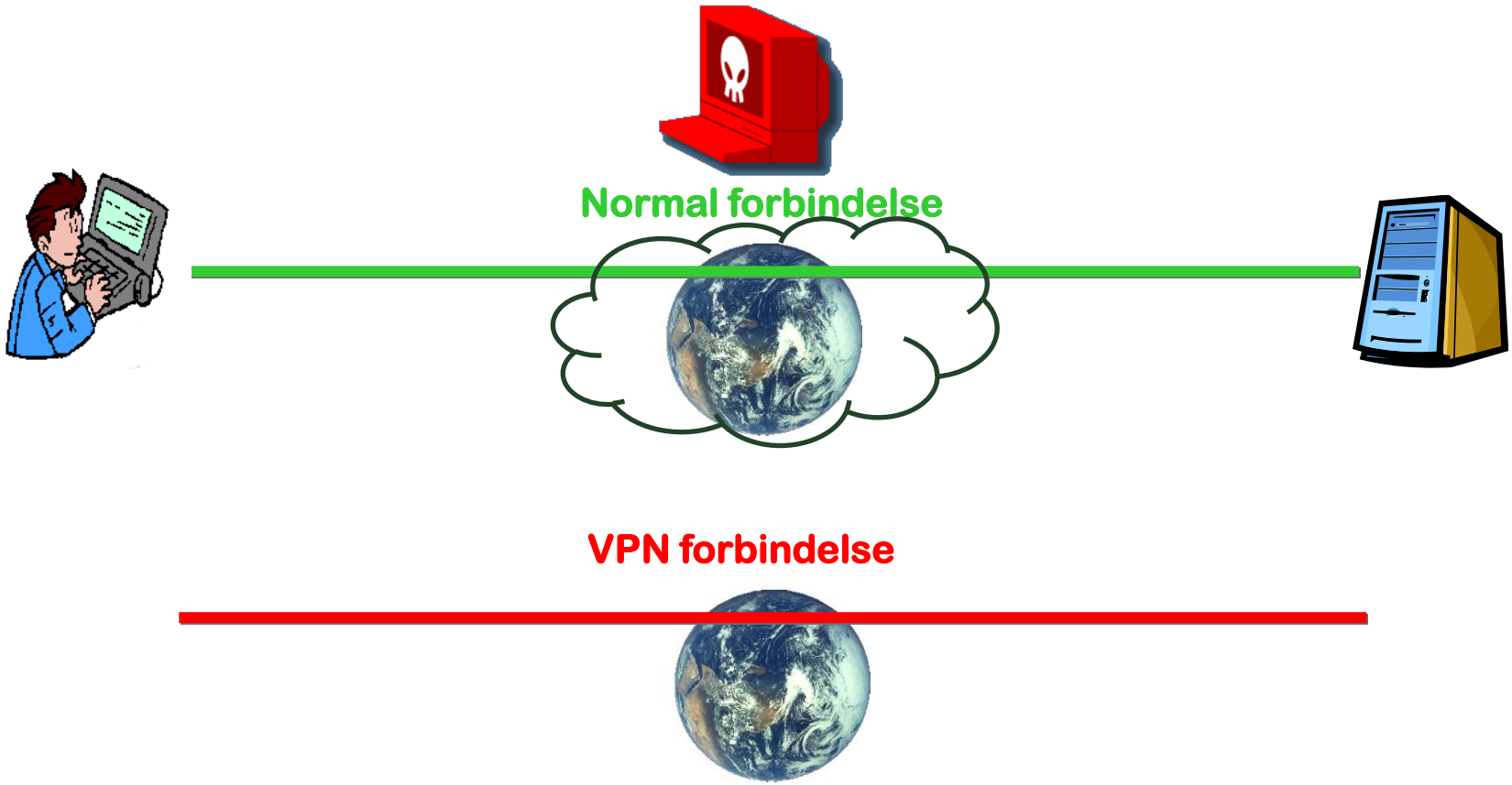
Normal TCP/IP packets are plaintext

The full packet content (header plus payload) is visible to every party with access to the packet stream, and alterable by any inline party (all intervening routers, switches, gateways, and service provider equipment)

For protection, one idea is to encrypt entire packets at origin devices before network transmission

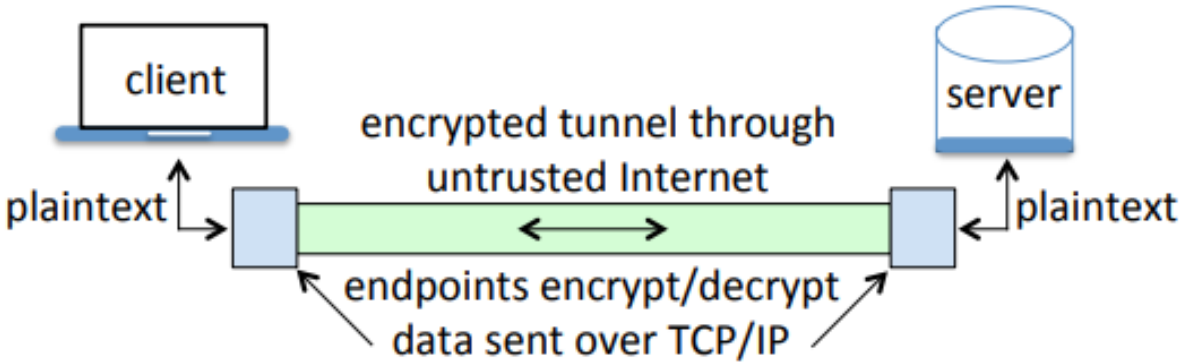
VPN

VPNs encrypt traffice between you and the VPN endpoint



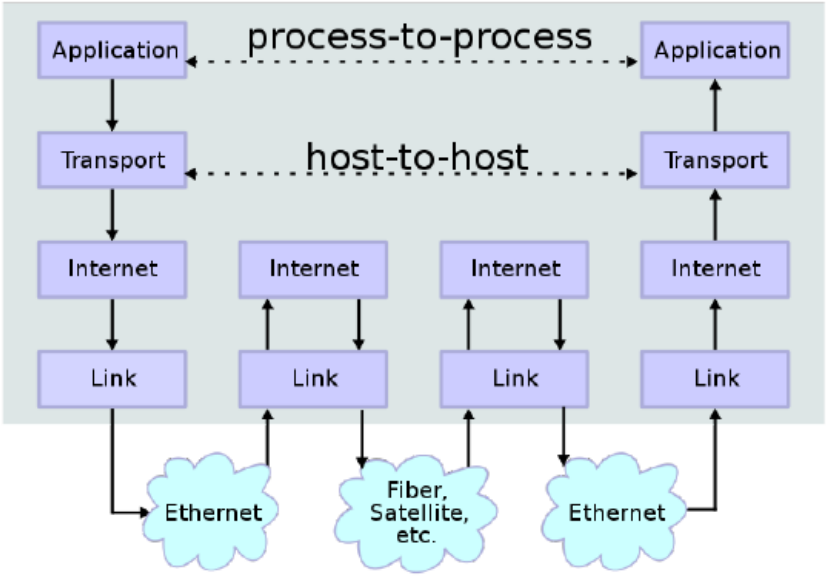
VPN

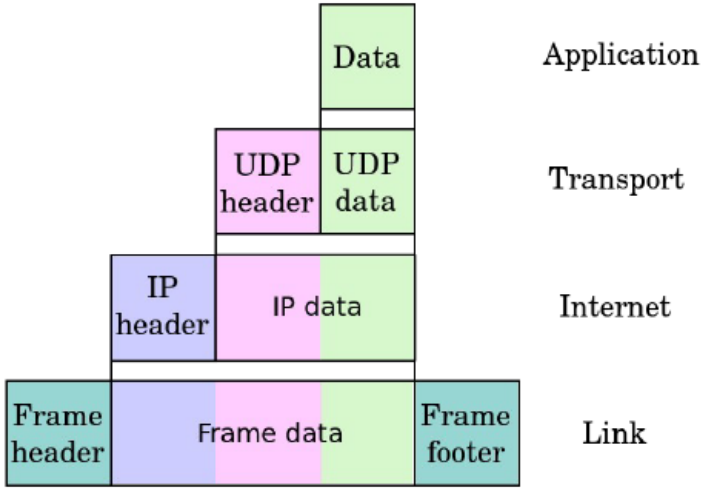
Encrypted connection between two networks



Tunnels

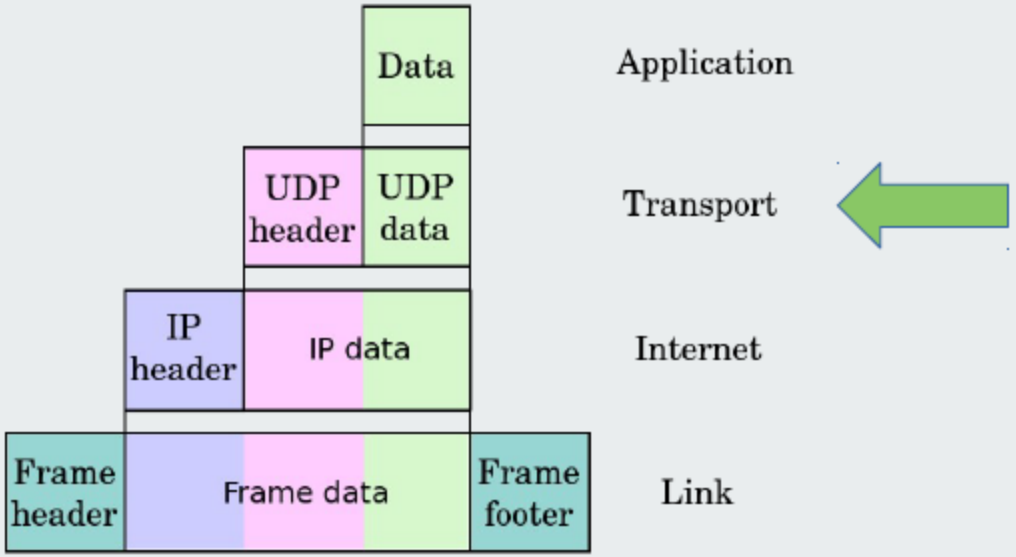
Where to encrypt?





Tunnels

The transport layer



Tunnels

SSL/TLS

Transport Layer Security (TLS), and its now-deprecated predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to:

"Provide a secure channel between two communicating peers" [RFC 8446 TLS 1.3]

SSL and TLS protocols

Protocol	Published	Status
SSL 1.0	Unpublished	Unpublished
SSL 2.0	1995	Deprecated in 2011 (RFC 6176)
SSL 3.0	1996	Deprecated in 2015 (RFC 7568)
TLS 1.0	1999	Deprecation planned in 2020[11]
TLS 1.1	2006	Deprecation planned in 2020[11]
TLS 1.2	2008	
TLS 1.3	2018	

Security goals of TLS

Specifically, the secure channel should provide the following properties:

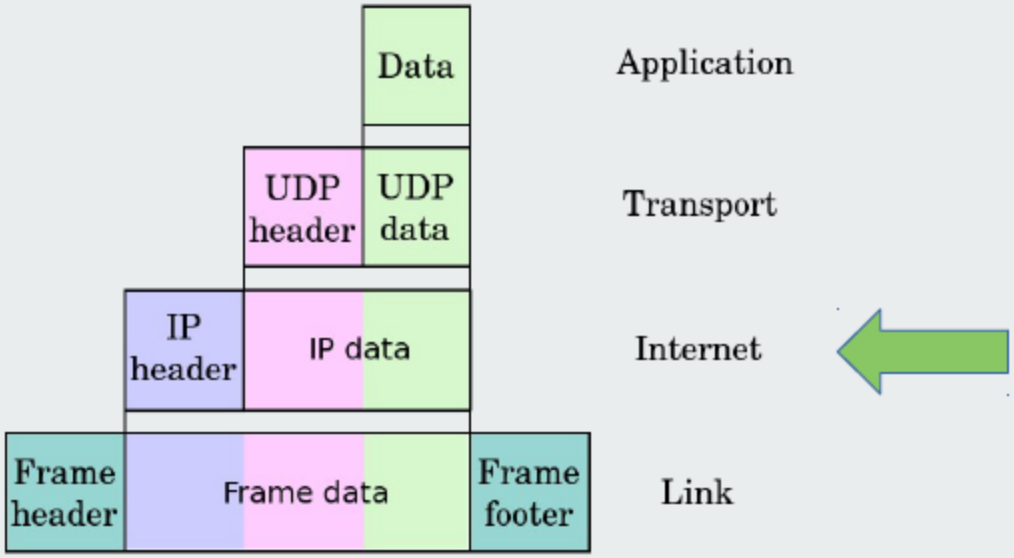
Authentication: The server side of the channel is always authenticated; the client side is optionally authenticated.

Confidentiality: Data sent over the channel after establishment is only visible to the endpoints.

Integrity: Data sent over the channel after establishment cannot be modified by attackers without detection.

Tunnels – network layer seurity

The Internet layer



IP-Sec VPN

Encrypted connection:
host-host
Network-network, host-network

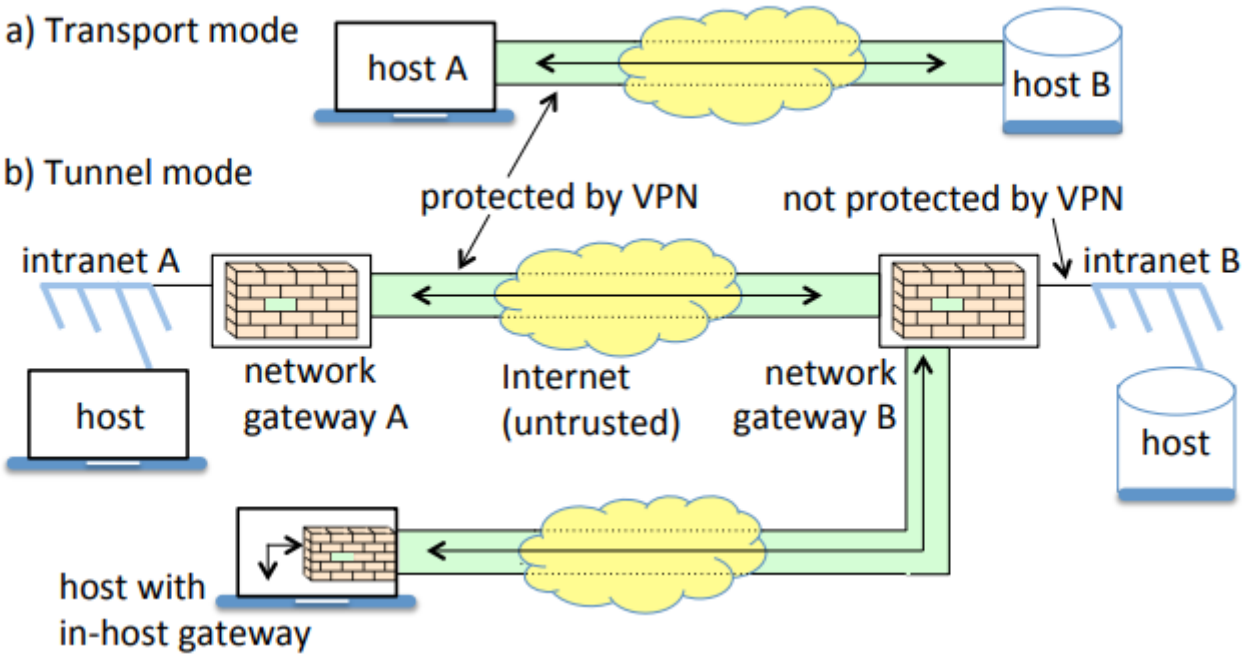
VPN design	VPN architecture	Notes and use cases
transport mode	host-to-host VPN	provides end-to-end security (VPN endpoints are final destination)
tunnel mode	network-to-network	network gateways add/remove VPN security (no VPN protection internal to gateway)
	host-to-network	for remote host access to enterprise (in-host gateway adds/removes VPN security)

Table 10.3: VPN designs and architectures. See Fig. 10.9 for illustrations.

Note that transport mode cannot be used if one endpoint is a network, as the resulting IPsec packet has only one IP header thus there would be no IP address available for a second-stage delivery

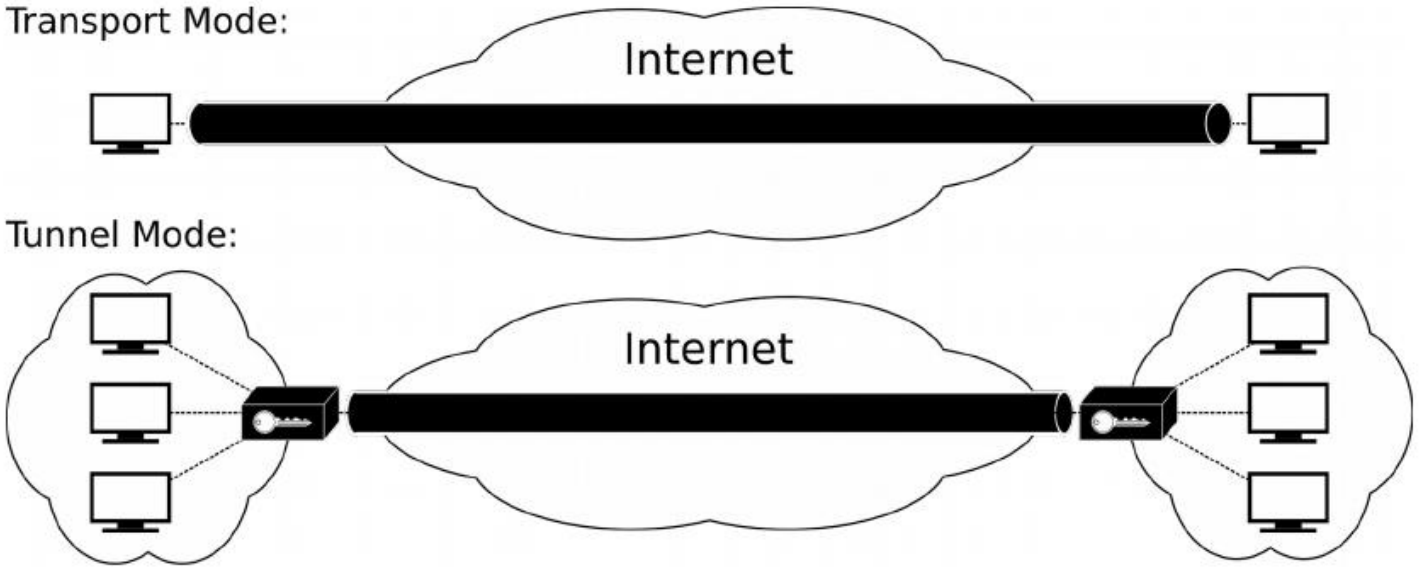
VPN

Transport mode and tunnel mode



Tunnels

IPSec – Transport or tunnel mode



No end-to-end security

Tunnels

IPSec – AH, ESP, SA

Authentication Header (AH)

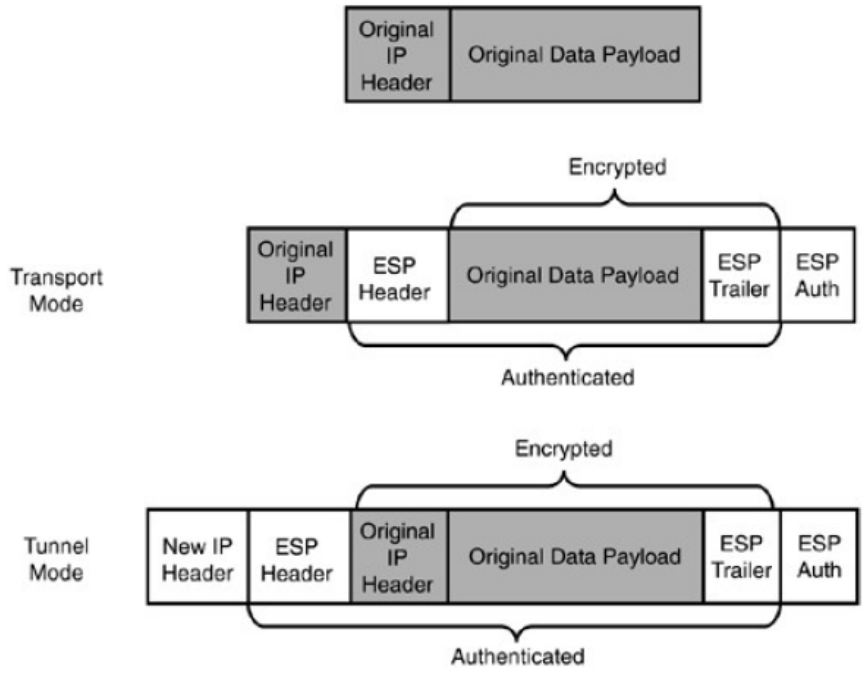
- Integrity and authentication

Encapsulating Security Payload (ESP)

- Confidentiality

Security Association

- Details on ciphers, keys, lifetime, etc.
- One directional

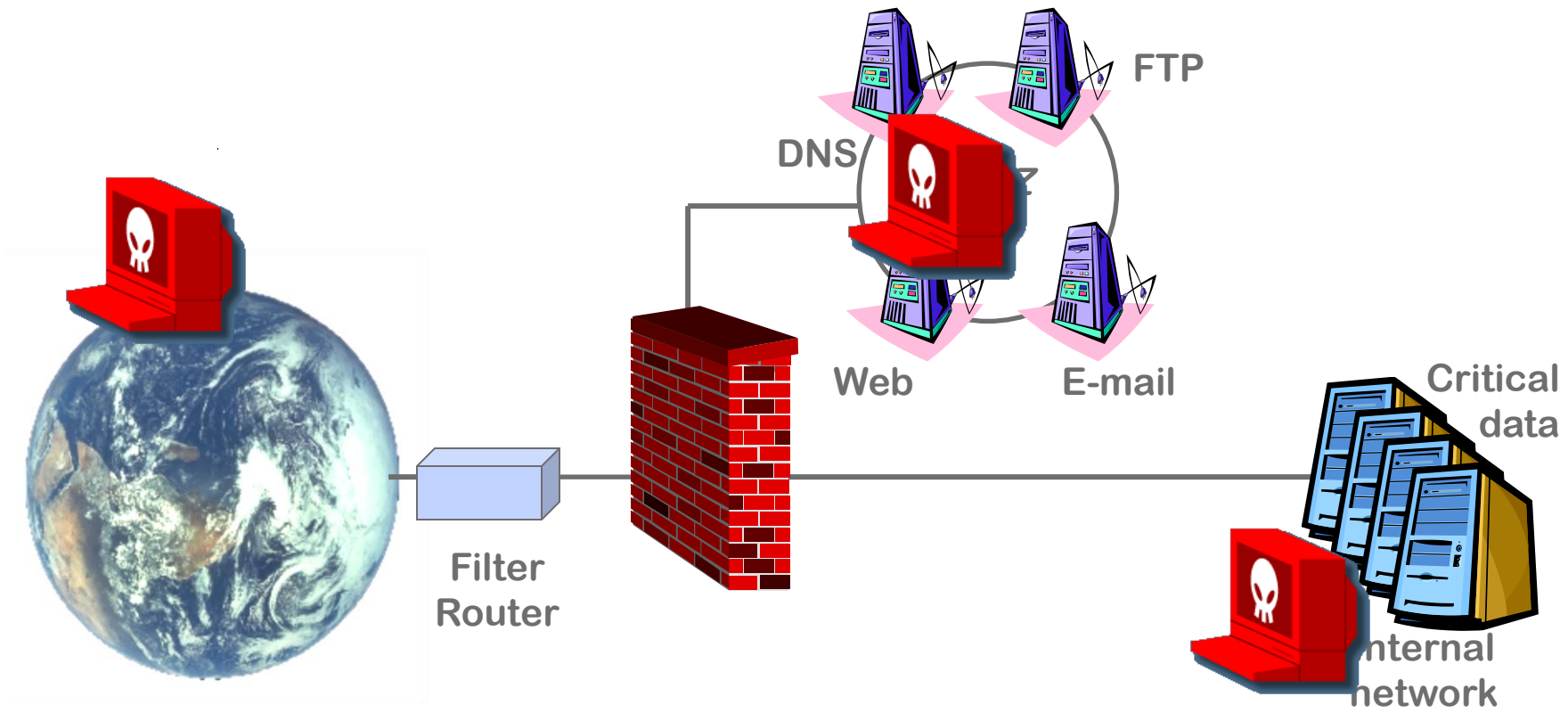


Pause

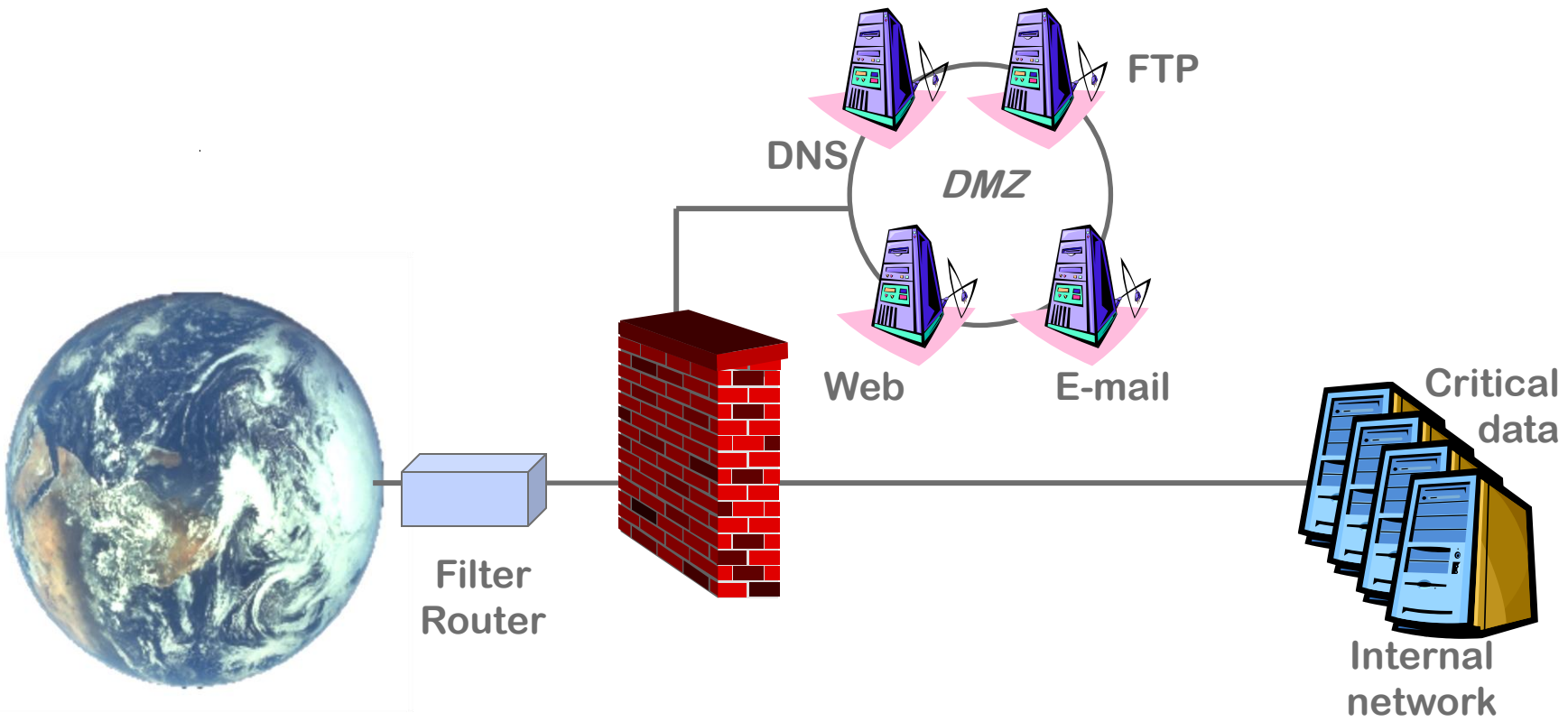

SECURITY CHECK
VISA
MasterCard
Is there your card in the hackers database?
You can easily check here, just enter your card info:
Card number:
- - -
CVC@ (CW2):
Check!

Common security issues (IT focus)

3 major areas of attack



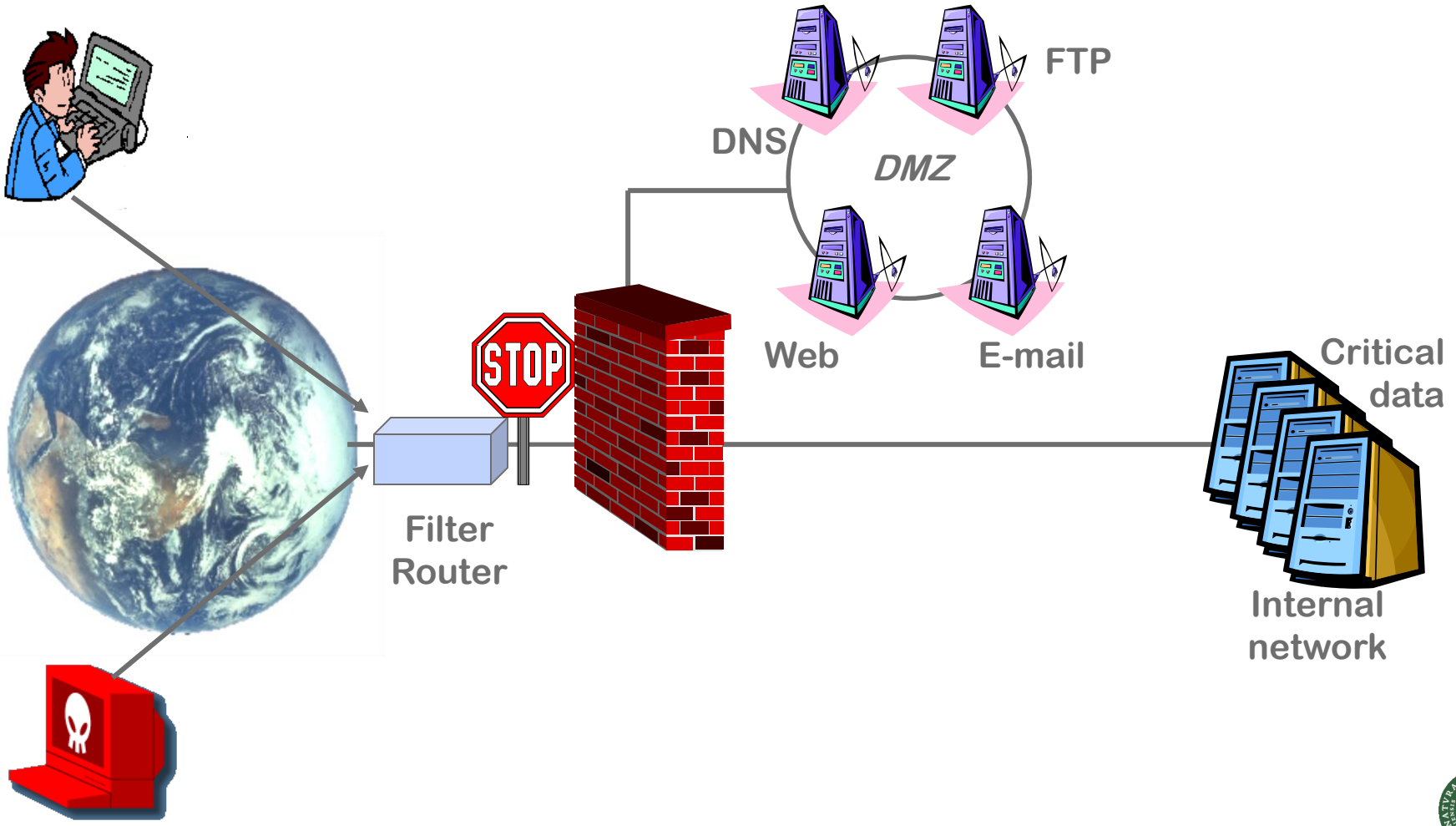
The network


FTP
DNS
DMZ
Web
E-mail
Critical data
Filter Router
Internal network

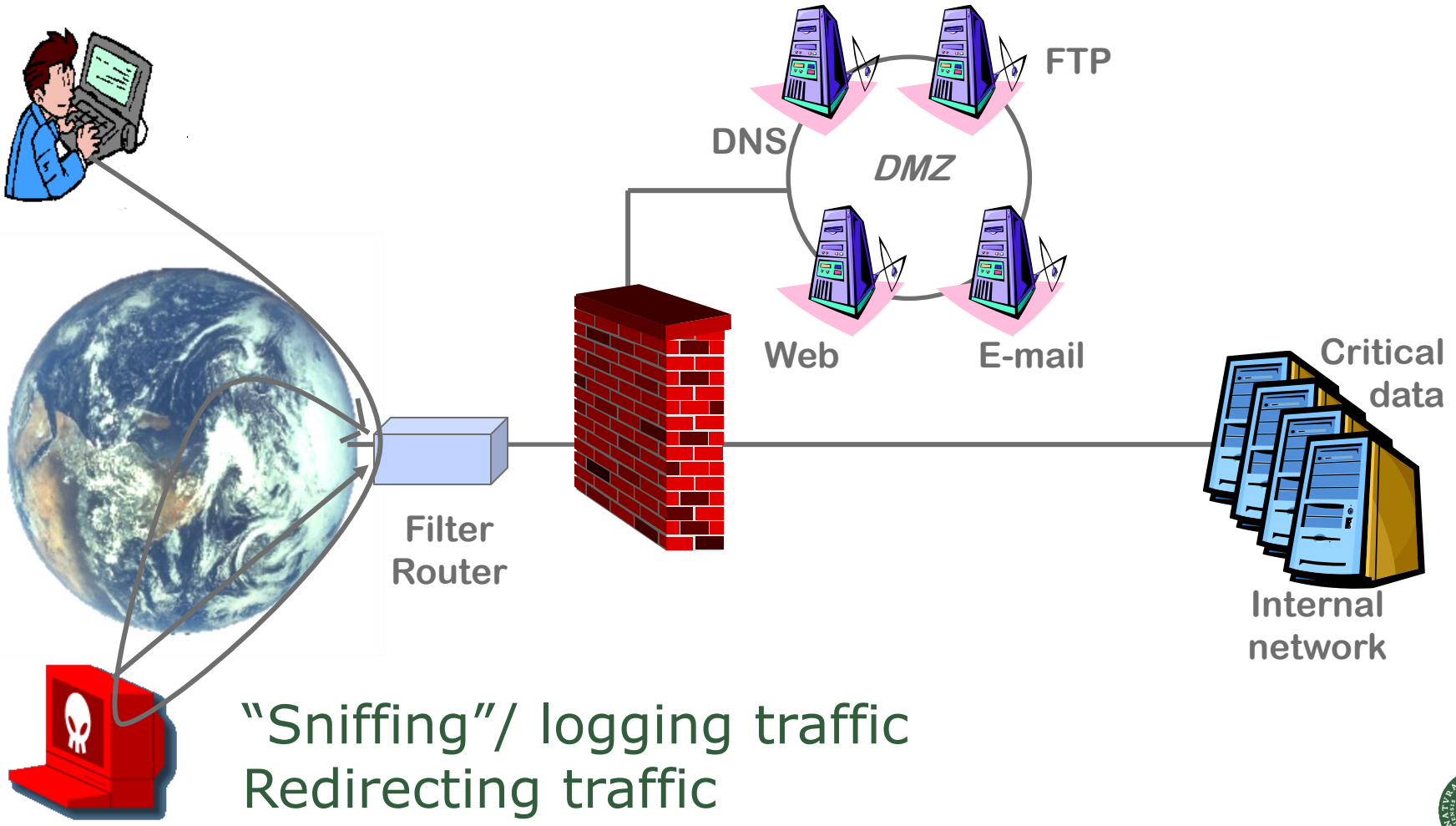
Typical router problems

- Too many open ports (access or DoS)
- Router default accounts and bad passwords

Router problems - consequences

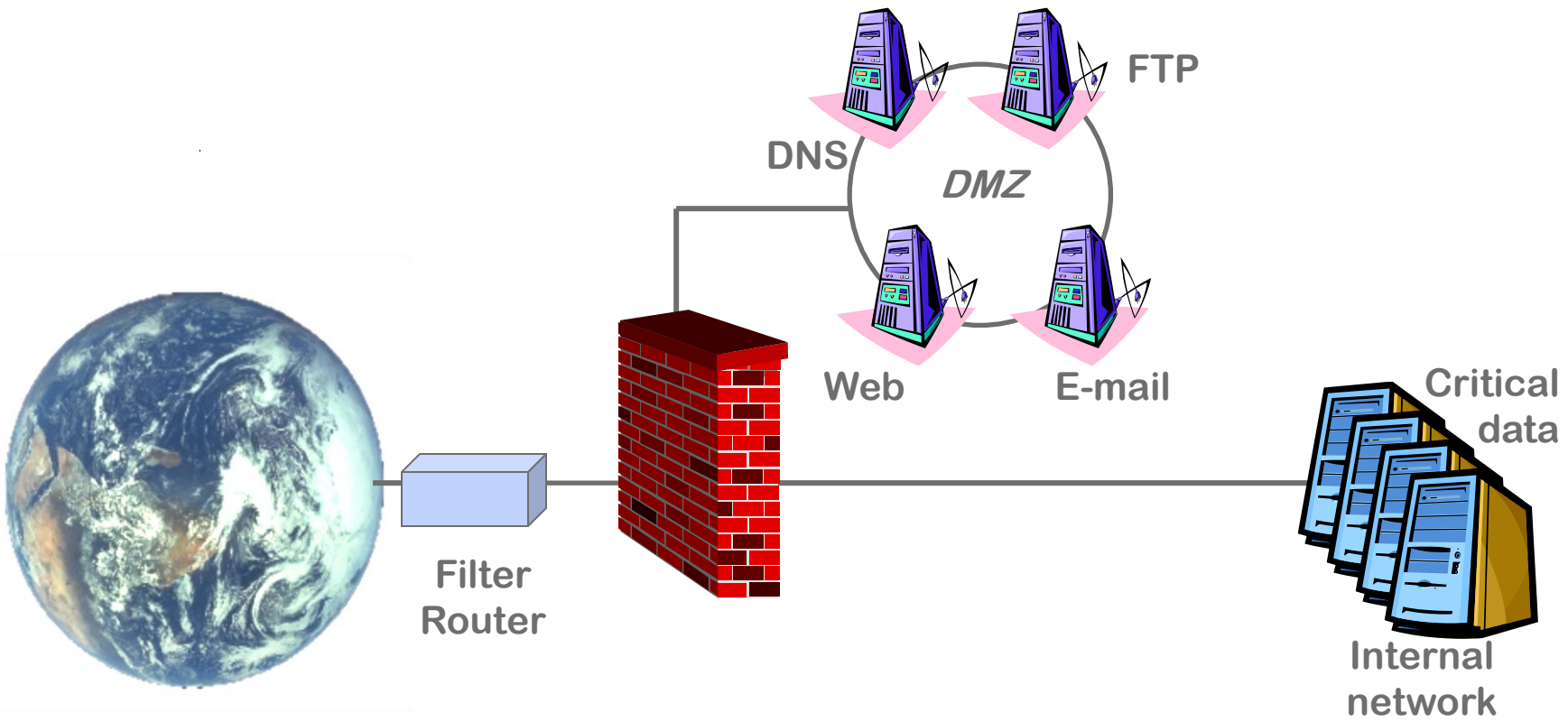


Router - consequences

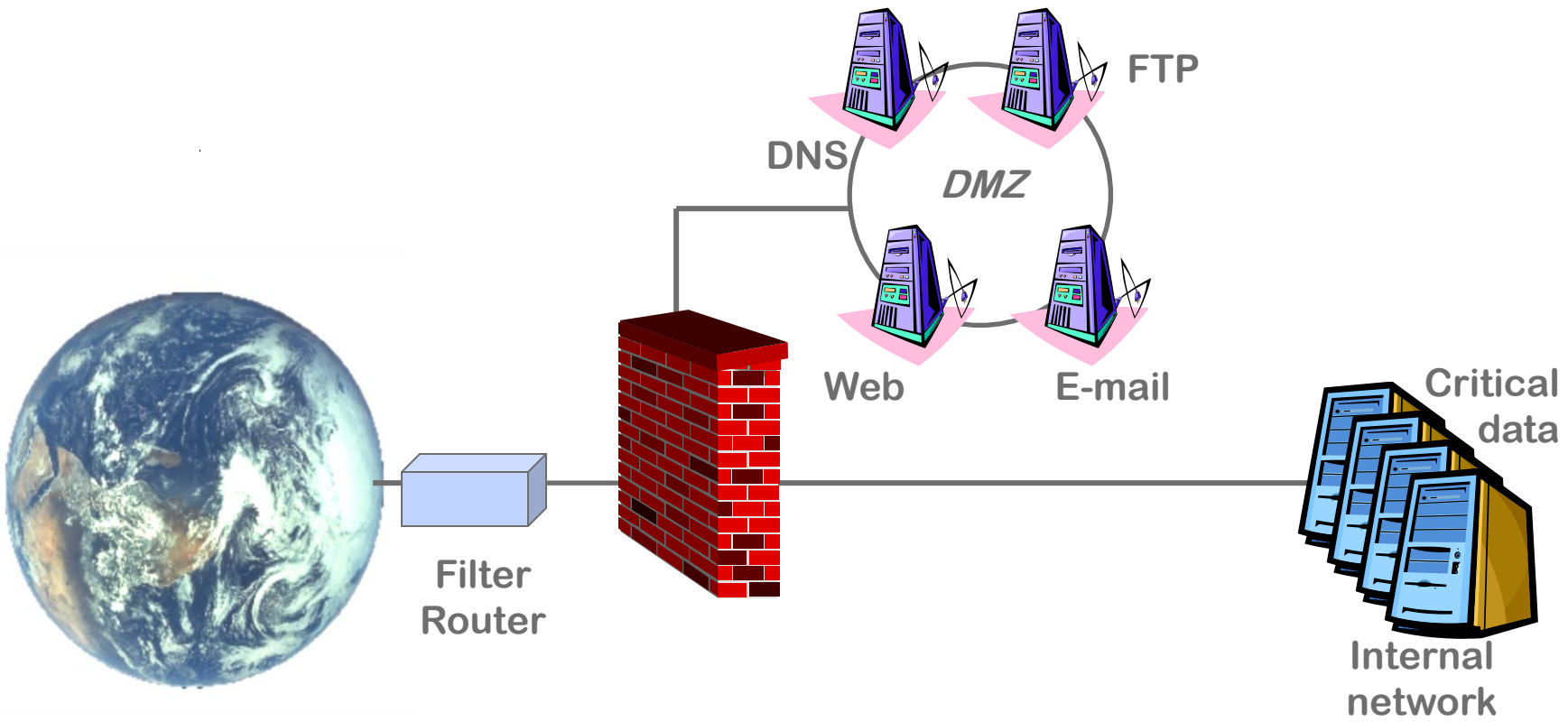


"Sniffing"/ logging traffic
Redirecting traffic

The network


FTP
DNS
DMZ
Web
E-mail
Critical data
Filter Router
Internal network

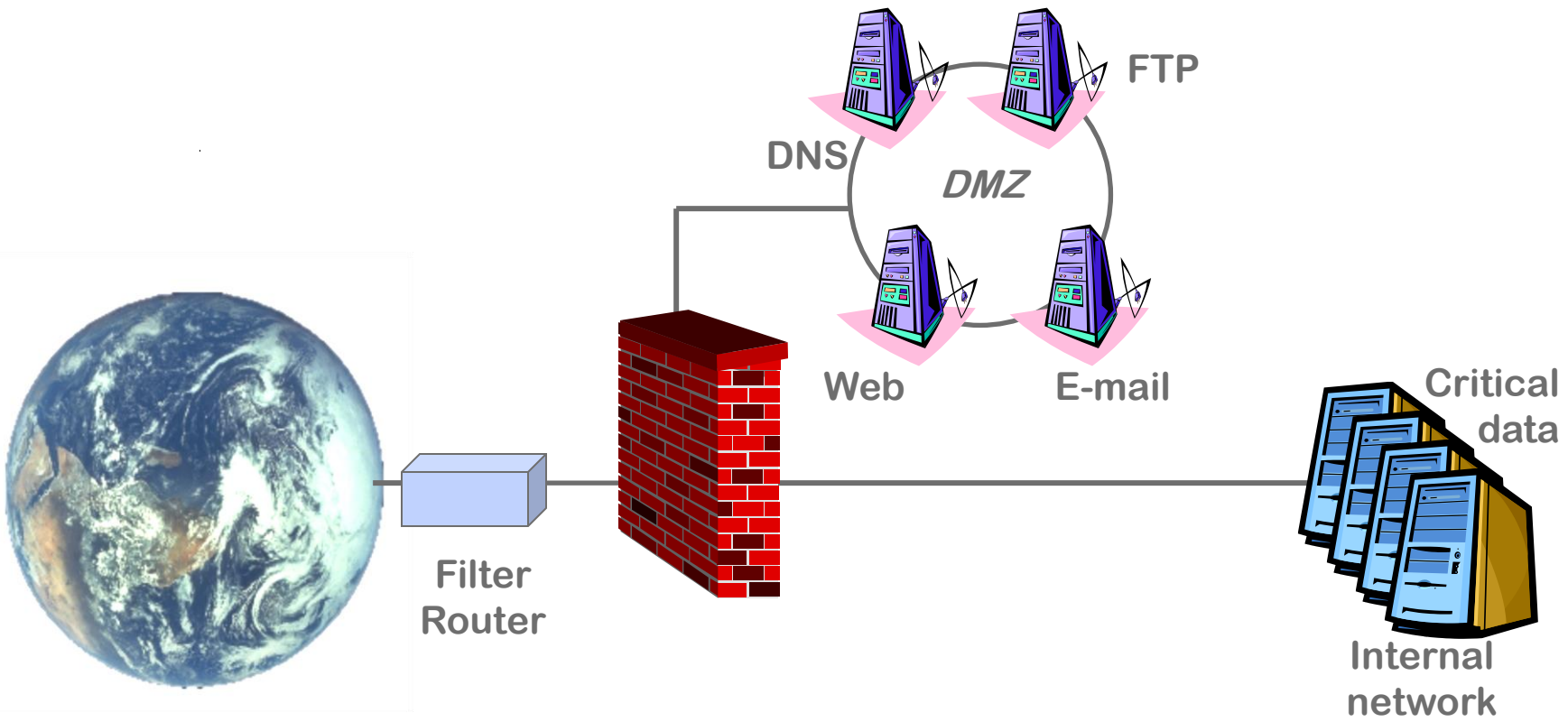
The network


FTP
DNS
DMZ
Web
E-mail
Critical data
Filter Router
Internal network

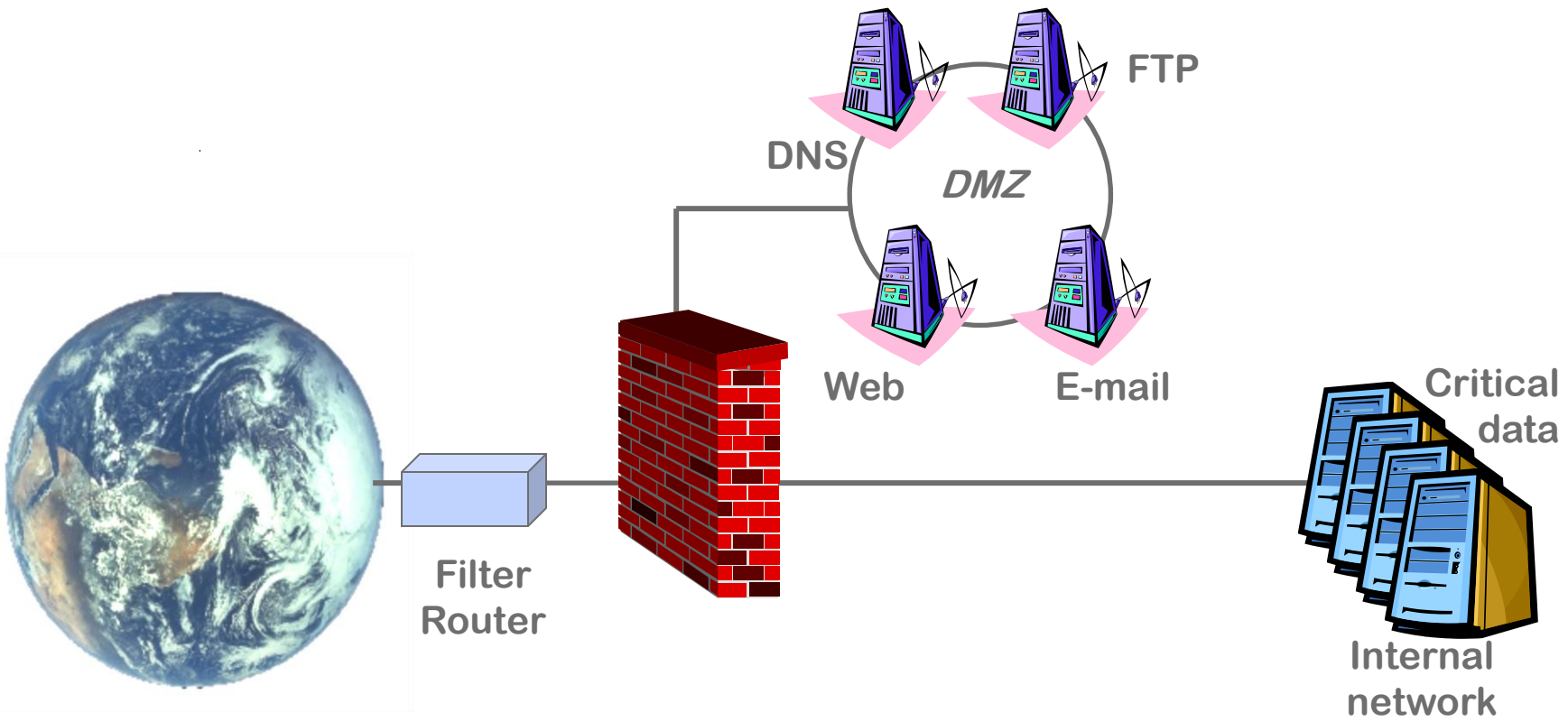
Typical firewall problems

- Mistakes in configuration
  (The FW does not protect as you think)
- Too many open ports (Access or DoS)
- Too many protocols allowed - ping etc.
- Changes in configuration never fixed
- Management services available on FW

Typical setup



Typical setup



Typical DNS issues

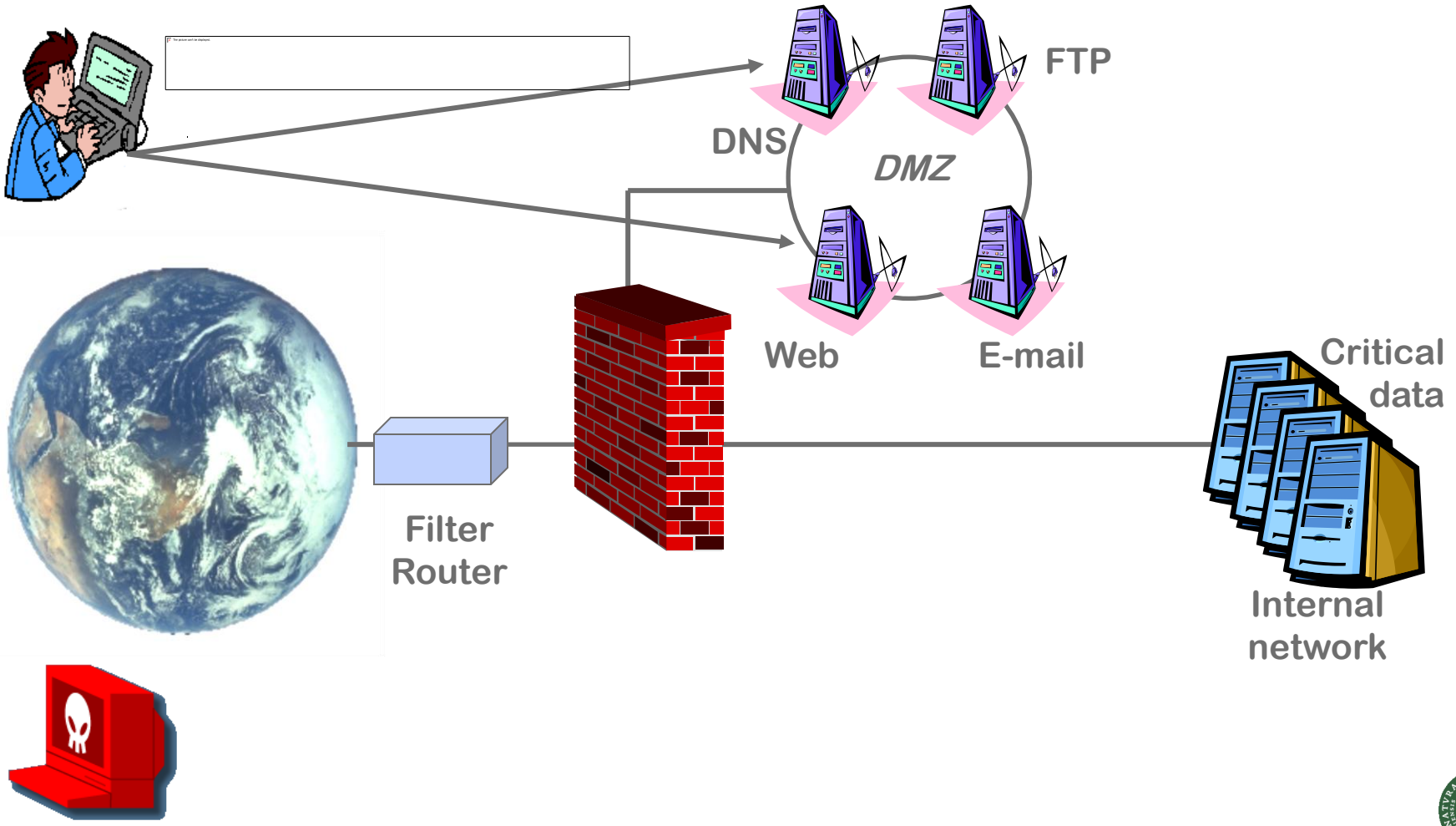
DoS

Re-direct traffic to other IP-addresses (Hijacking/Man-in-the-Middle)

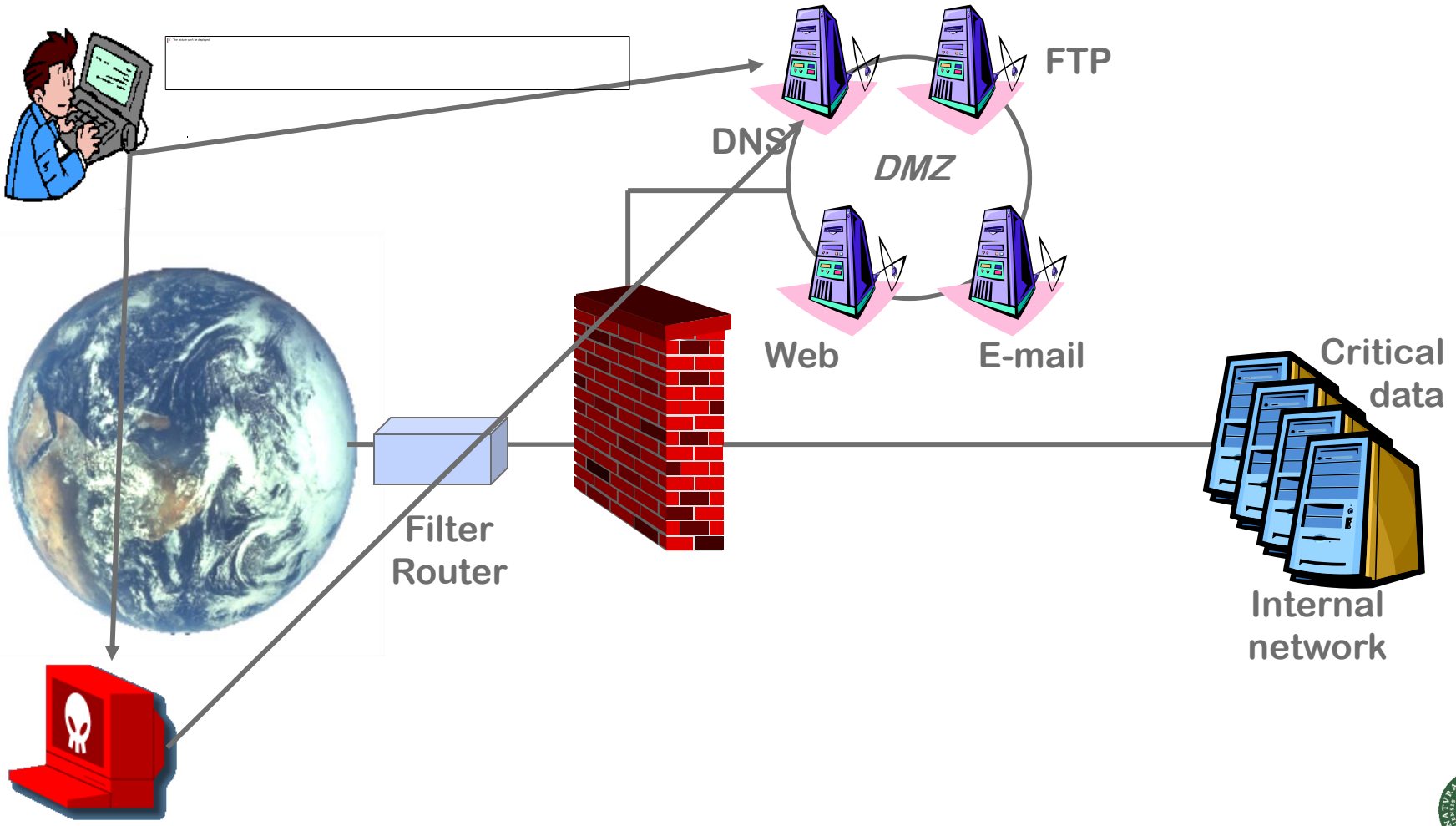
Execute commands on the server

Stepping Stone

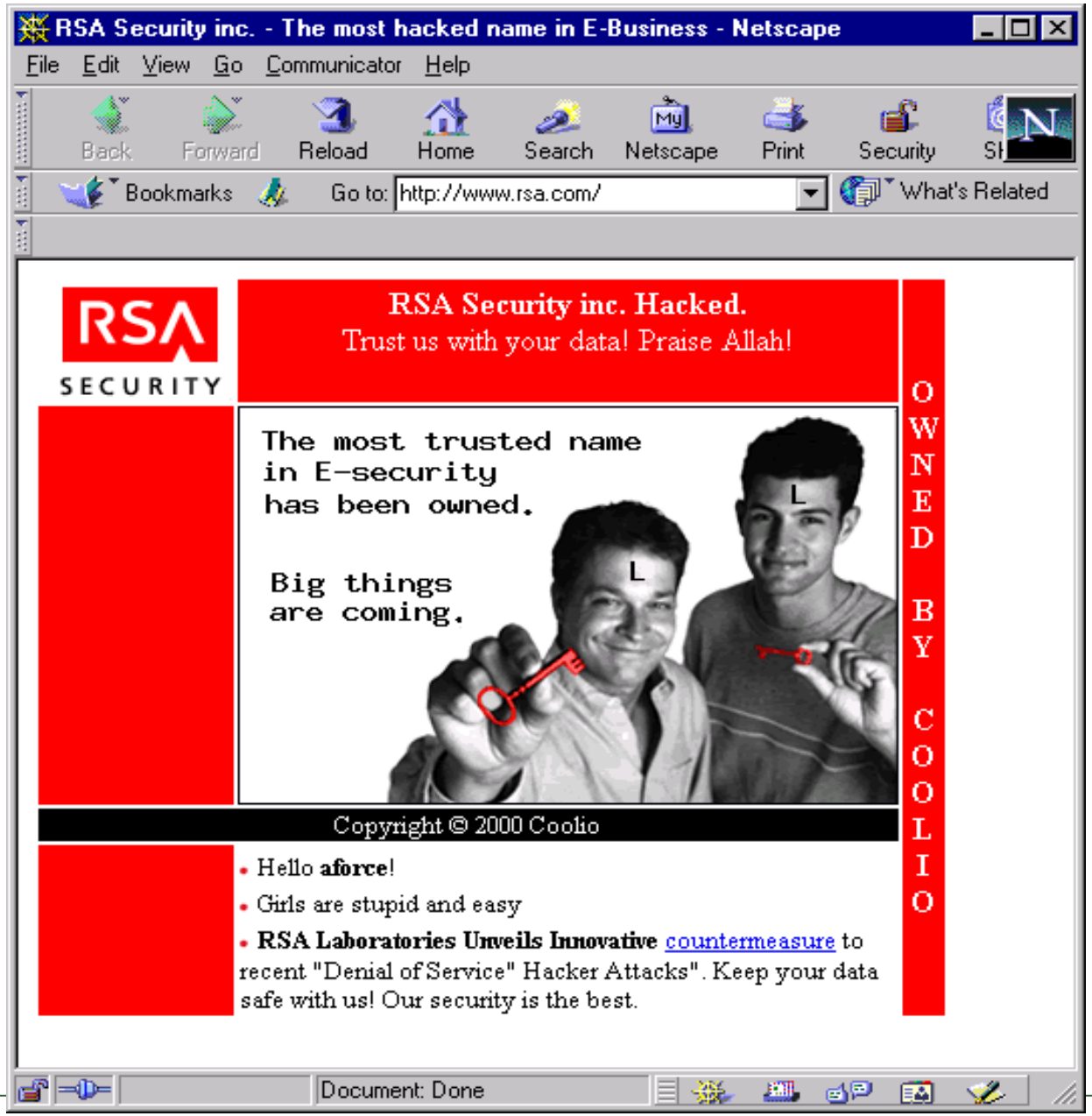
DNS problems - consequences



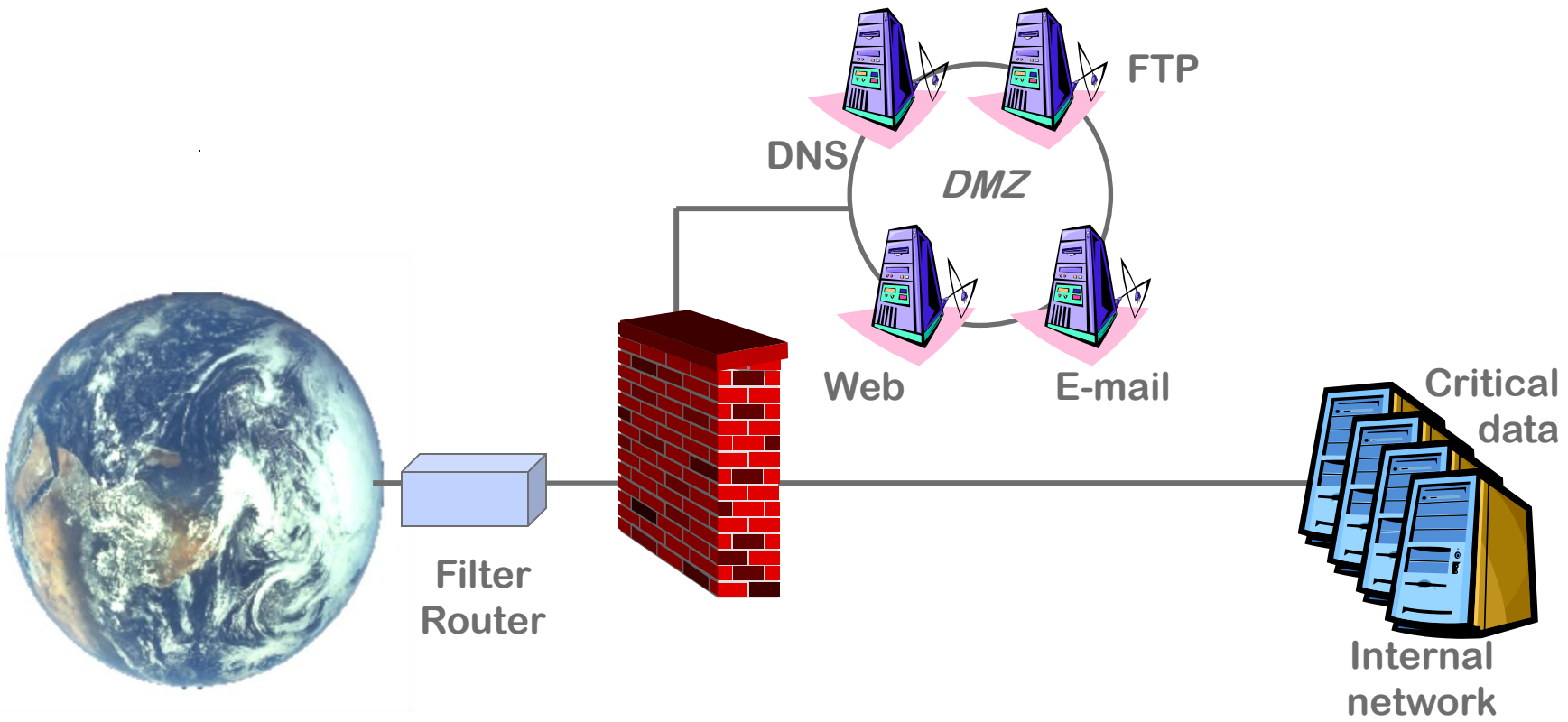
DNS problems - consequences



DNS - Case Story: RSA DNS Hijacking



Typical setup



Consequences

- Defacements - the website is the company's 'face' to the outside
- Attack server / Distribution server (legal consequences)
- Stepping Stone to internal/other servers

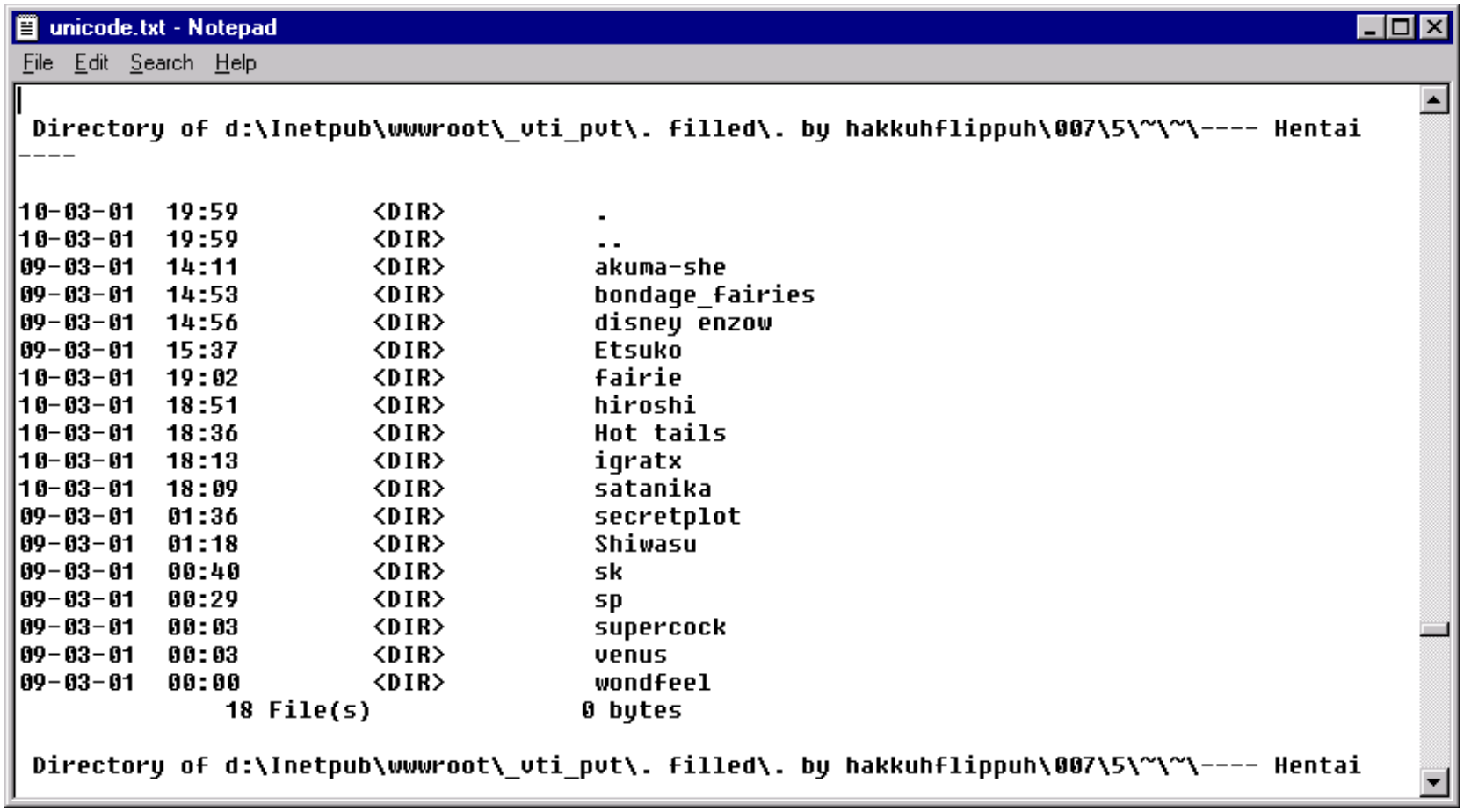
Warez server - 4.5GB data

unicode.txt - Notepad

File Edit Search Help

```
 Directory of d:\Inetpub\wwwroot\_vti_pvt\. filled\. by hakkuhflippuh\007\5\~

08-03-01  15:04         <DIR>          .
08-03-01  15:04         <DIR>          ..
11-04-01  16:13         <DIR>          ~
               3 File(s)              0 bytes

 Directory of d:\Inetpub\wwwroot\_vti_pvt\. filled\. by hakkuhflippuh\007\5\~\~

11-04-01  16:13         <DIR>          .
11-04-01  16:13         <DIR>          ..
08-03-01  20:37         <DIR>          ---- Anime ----
08-03-01  20:05         <DIR>          ---- Appz ----
10-03-01  19:59         <DIR>          ---- Hentai ----
25-03-01  15:52         <DIR>          ---- Mp3 ----
13-04-01  21:15         <DIR>          ---- old games ----
11-04-01  16:14             1.000.000 1.mb
               8 File(s)      1.000.000 bytes

 Directory of d:\Inetpub\wwwroot\_vti_pvt\. filled\. by hakkuhflippuh\007\5\~\~\---- Anime
----

08-03-01  20:37         <DIR>          .
08-03-01  20:37         <DIR>          ..
09-03-01  04:36         <DIR>          Escaflowne - The Movie
```

Warez server



Security architecture

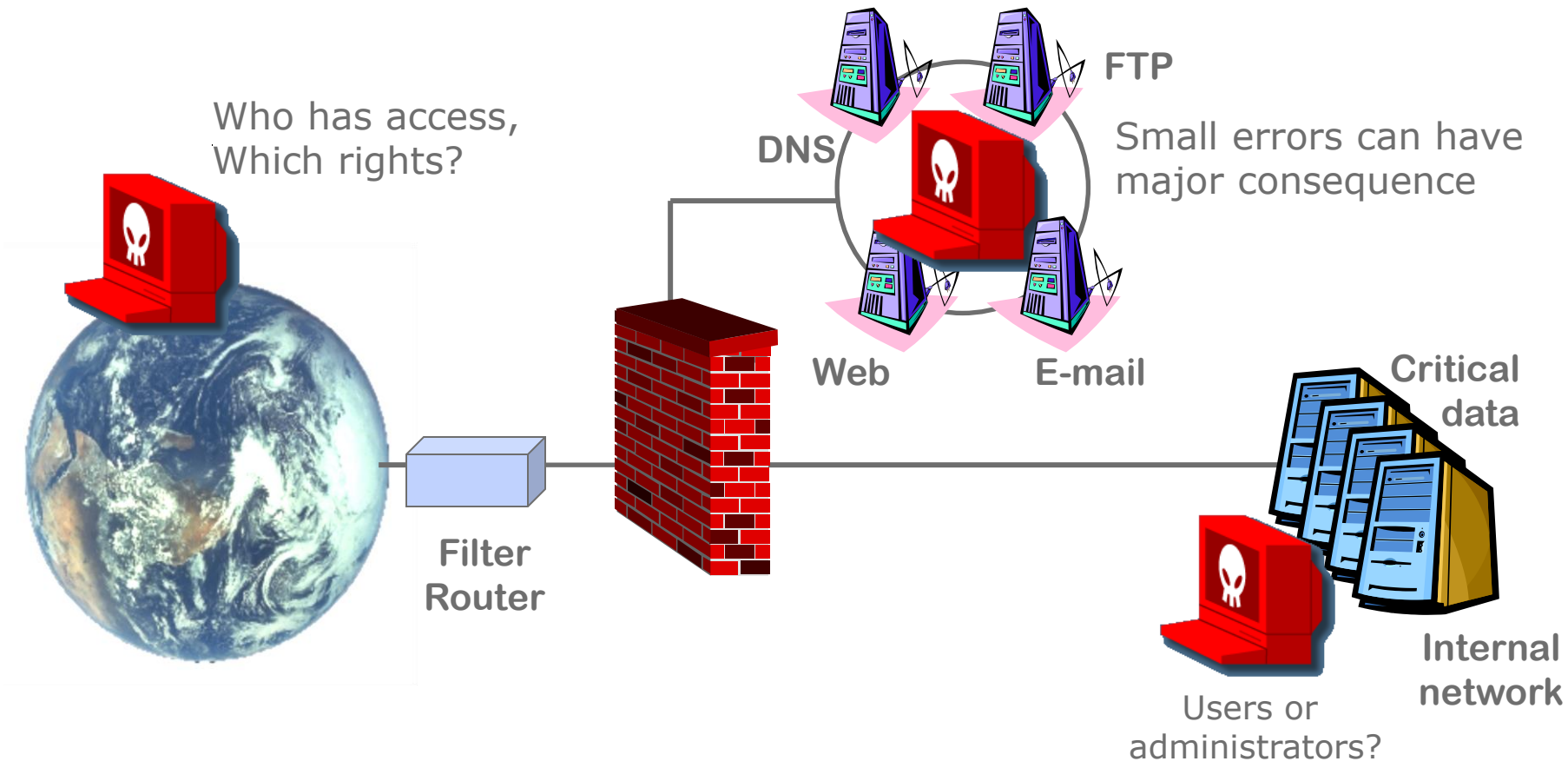
- Minimize attack surface – provide as few areas of attack as possible
- Realize where it is possible to attack
- Understand the attackers – and make it difficult for them
- Segment and separate
- Defence in depth – many layers of security
- Jump servers
- Monitor and log, IDS
- Handle security breaches and security incidents
- Test the security

Security architecture

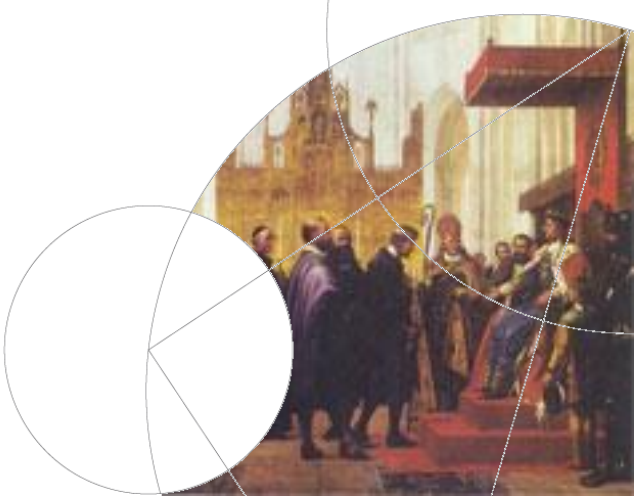
- Hardening – remove all unnecessary tools, services, protocols etc.
- Patchning
- Konfiguration
- Lowest and fewest possible rights
- User awareness

IT Security – start from the outside and zoom in

3 areas of attack

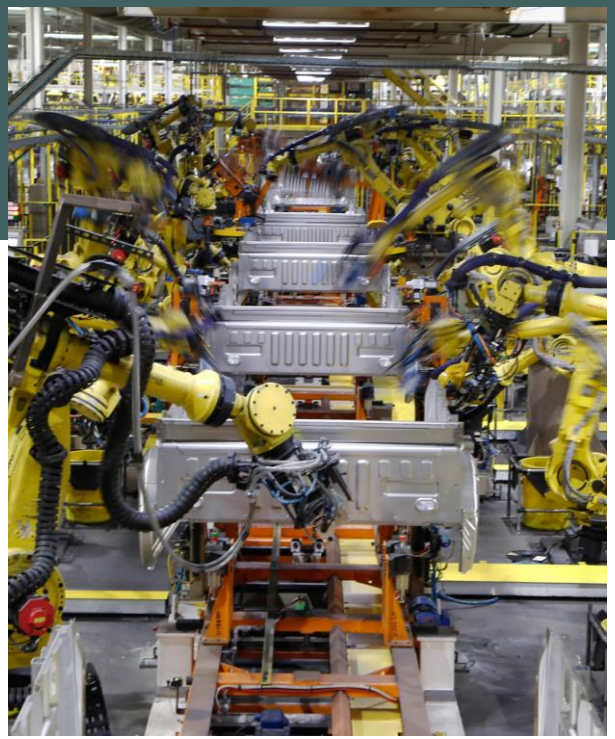


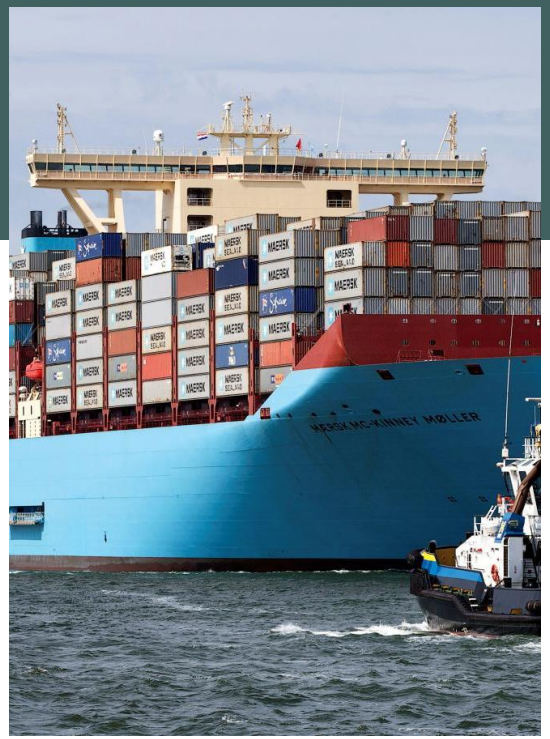
OT/SCADA



What is Operational Technology (OT) Security?!

WHERE CYBER MEETS THE PHYSICAL WORLD



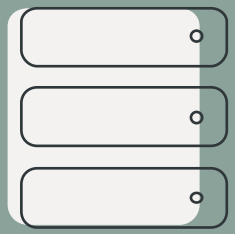


Contrasting OT and IT

INFORMATION TECHNOLOGY (IT) VS. OPERATIONAL TECHNOLOGY (OT)

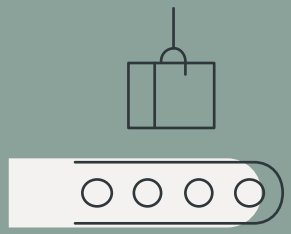
IT

Data and the flow of digital information



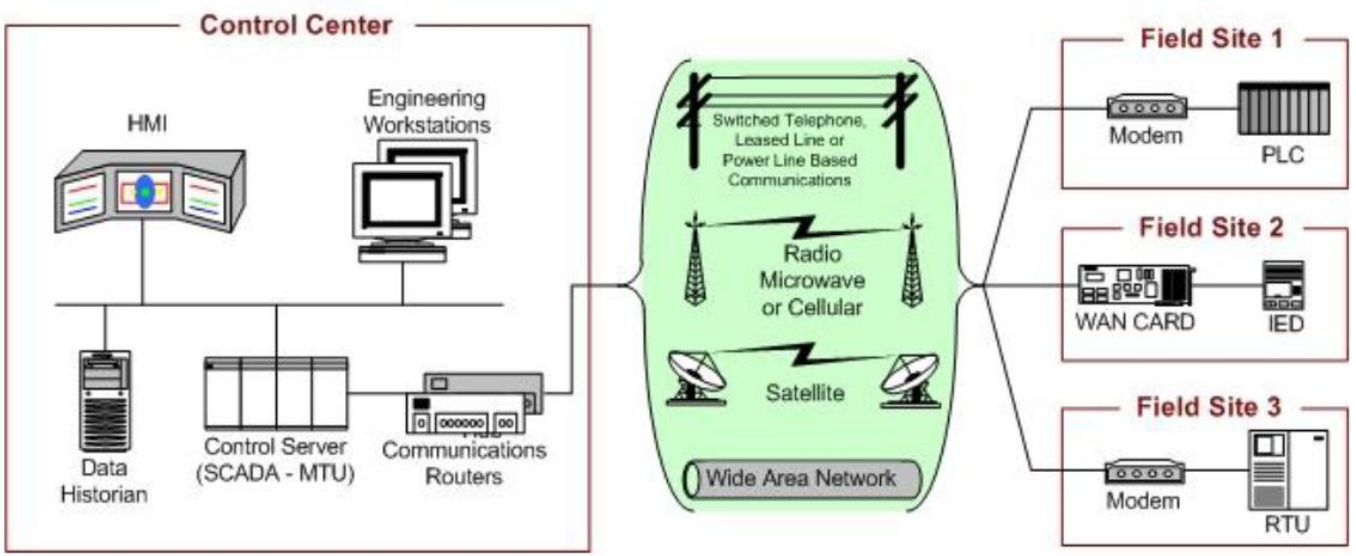
OT

Operation of physical processes and the machinery used to carry them out



OT – Operational Technology

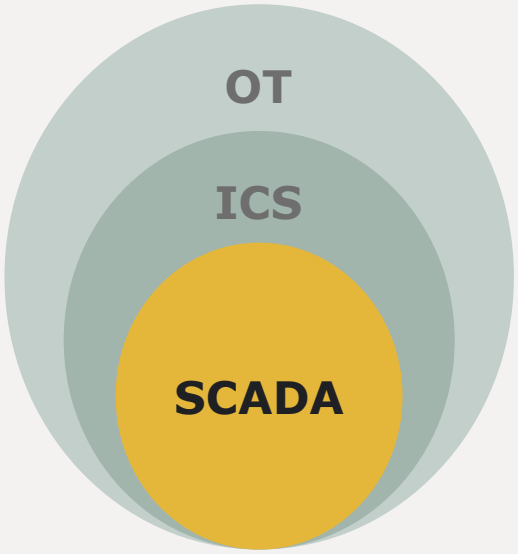
OT is "**technology that interfaces with the physical world**". Includes Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS)



Internet?

Figure 2-2. SCADA System General Layout

Making sense of the conceptual jungle

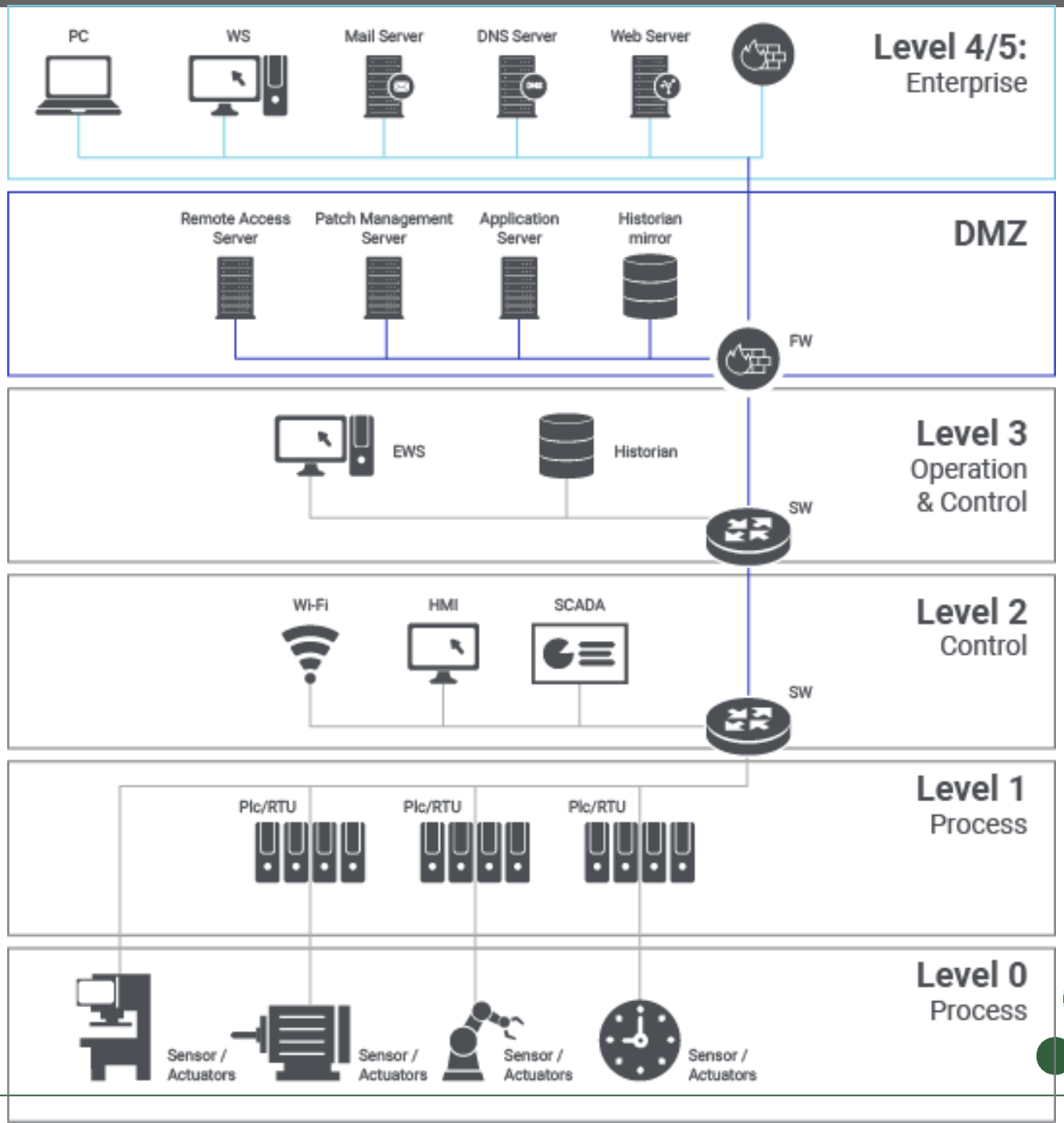


Operational Technology (OT)
The hardware and software used to control industrial processes

Industrial control systems (ICS)
ICS is a major subset within the OT Sector and used to control industrial processes such as manufacturing, product handling, production, and distribution.

Supervisory Control and Data Acquisition (SCADA)
The hardware and software systems that allows control and monitoring of field devices at local or remote sites

Perdue


PC
WS
Mail Server
DNS Server
Web Server
Level 4/5:
Enterprise
Remote Access Server
Patch Management Server
Application Server
Historian mirror
DMZ
FW
EWS
Historian
Level 3
Operation & Control
SW
Wi-Fi
HMI
SCADA
Level 2
Control
SW
Plc/RTU
Plc/RTU
Plc/RTU
Level 1
Process
Sensor / Actuators
Sensor / Actuators
Sensor / Actuators
Sensor / Actuators
Level 0
Process

OT – Operational Technology

Originally completely isolated systems and networks

Perdue-model
But…

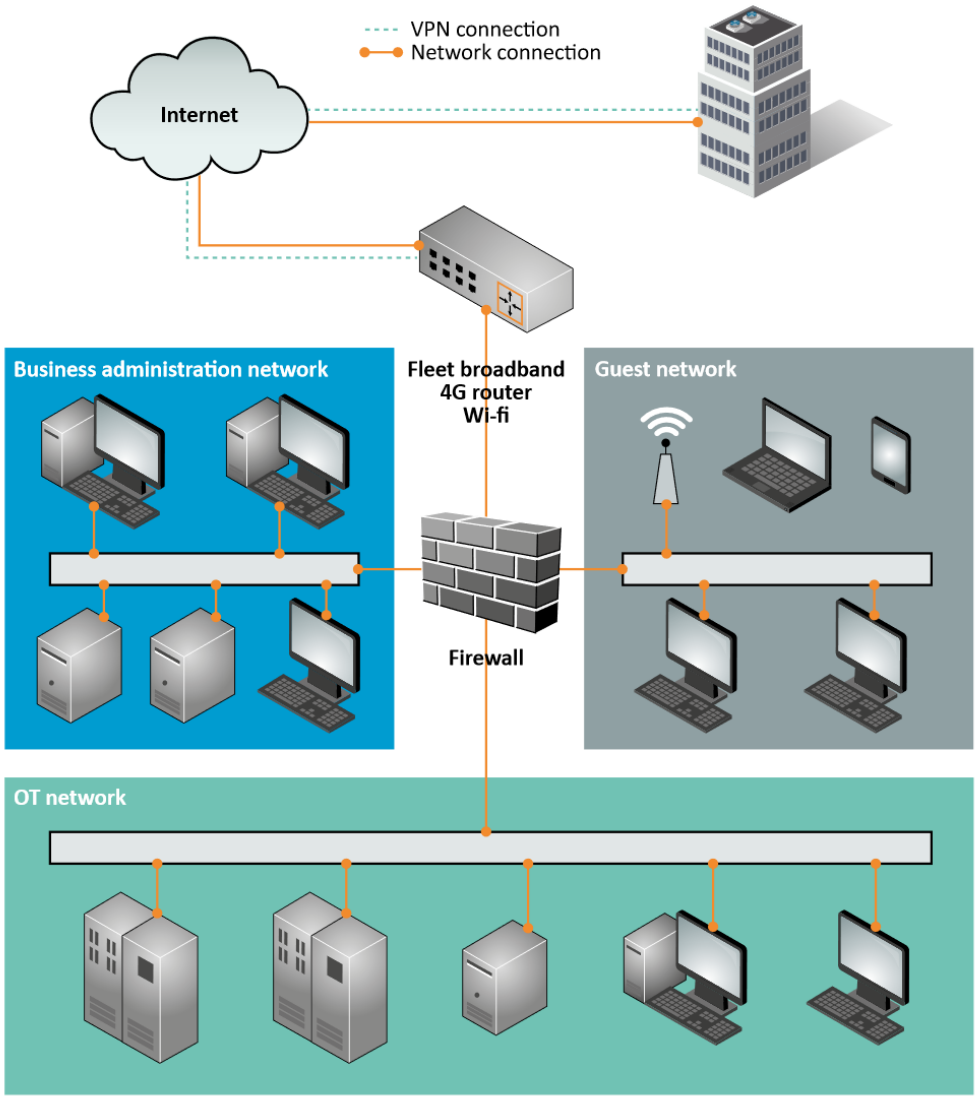


Figure 2: Example of an onboard network

OT – Operational Technology

Cyber security for IT has traditionally been concerned with **CIA** - Confidentiality, Integrity and Availability

OT priorities are often **safety**, **reliability** and **availability** - there are usually clearly *physical dangers* associated with OT failure or malfunction

"Business 4.0" and New world

Building an OT security program - getting the fundamentals right

Understand the risks
- OT loss impact
- OT vulnerability assessment
- OT security risk and compliance assessment

Mitigate Impact
- Establish OT governance
- Design, build, run and optimize an OT security setup
- Plan and implement OT Identity and Access Management (IAM) solutions
- Develop OT security incident detection & response

Extend visibility
- Conduct network discovery and security architecture review
- Conduct asset discovery and classification of assets
- Perform OT/ICS user access review

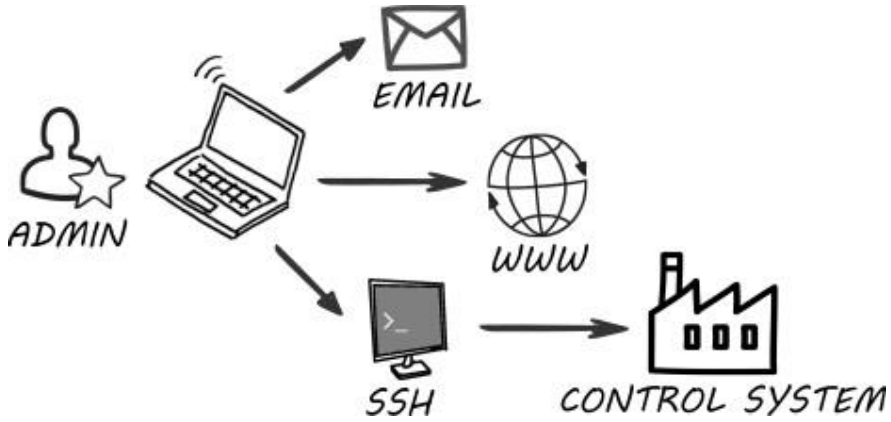
SECURING CONTINUED OPERATIONS

+

MAINTAINING SAFETY

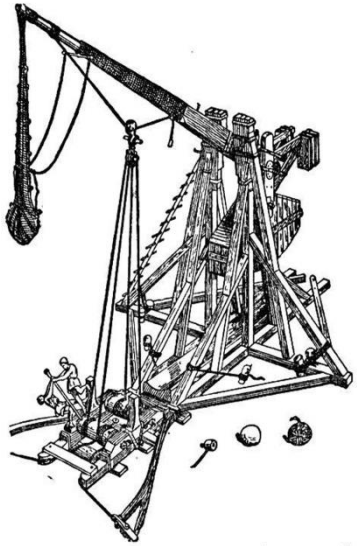
OT – Operational Technology - and also IT

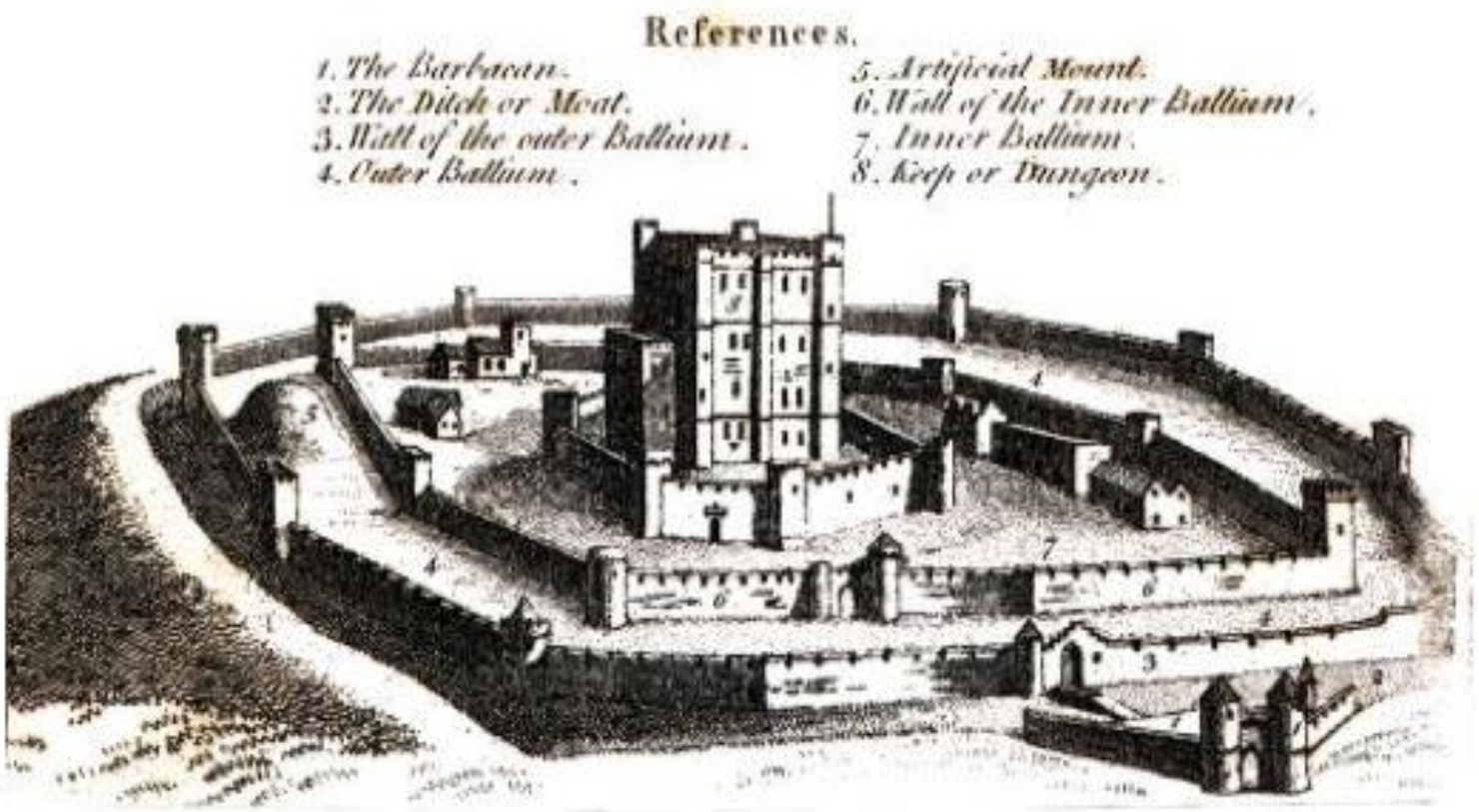
Browse-up
When administration of a system is performed from a device which is less trusted than the system being administered



Old School vs. New World

IT Security threats





Distribuerede netværk, login fra mange forskellige lokationer osv osv

Towards the cloud – and beyond

Many To One

Mange brugere
En enkeltstående
central server

I forgårs

One To One

En bruger
En computer

I går

One To Many

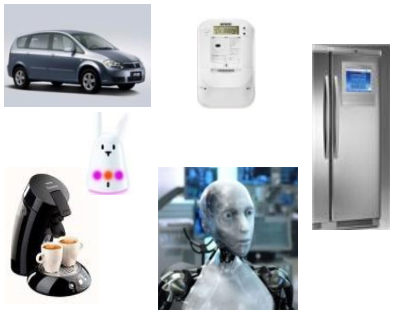
En bruger
Mange medier

I dag

Mobilitet

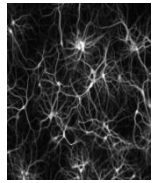
Machine To Machine

Many To Many



I morgen

Allesteds-nærværende



Neuro-
Nano-
technologier

I over-morgen

Towards the cloud – and beyond

Many To One

Mange brugere
En enkeltstående central server

I forgårs

One To One

En bruger
En computer

I går

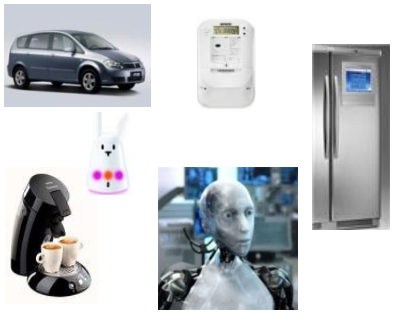
One To Many

En bruger
Mange medier

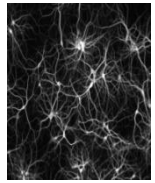
I dag

Machine To Machine

Many To Many



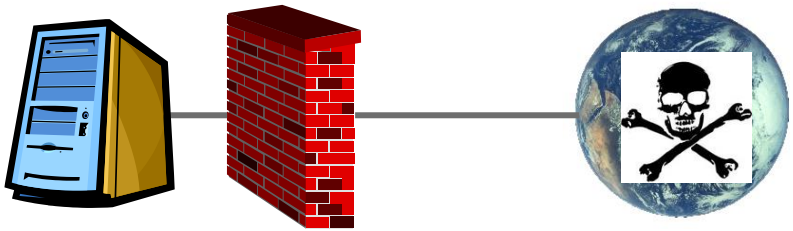
I morgen



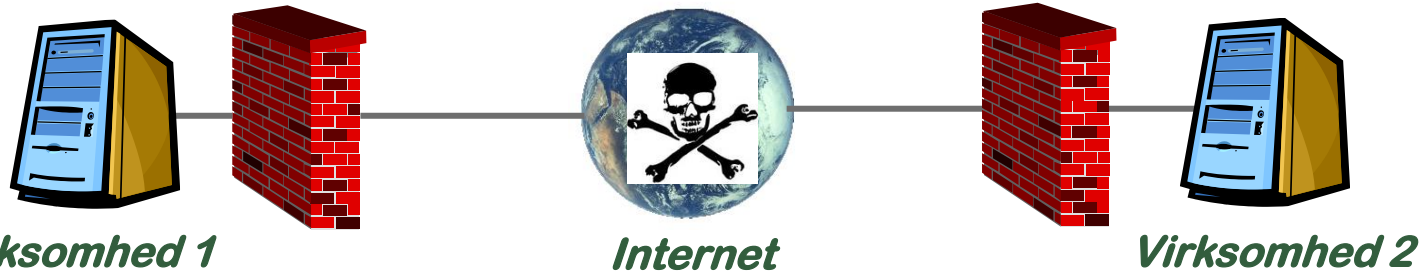
Neuro-
Nano-
technologier

I over-morgen

Inside-out



"I'm ok – but we can't trust the network"



"I'm ok, and you're ok – but we can't trust the network"

Traditional focus on perimeter (firewall, SSL, VPN etc.) and device control (antivirus and AD-password)

The same level of security everywhere?

Zentropa and Danish National Bank?

Same security culture for everyone internally?

New world

A major shift from thinking security

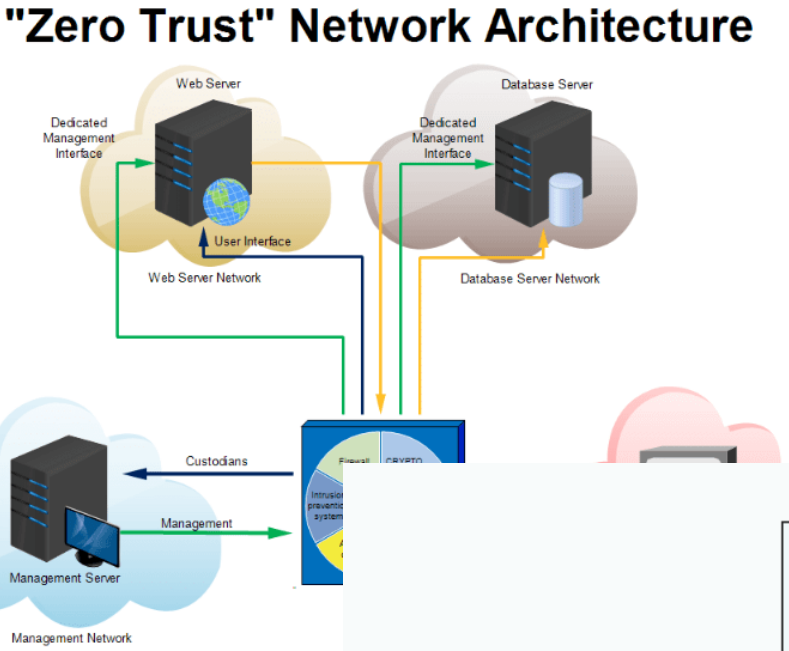
Inside-out  **Outside-in**

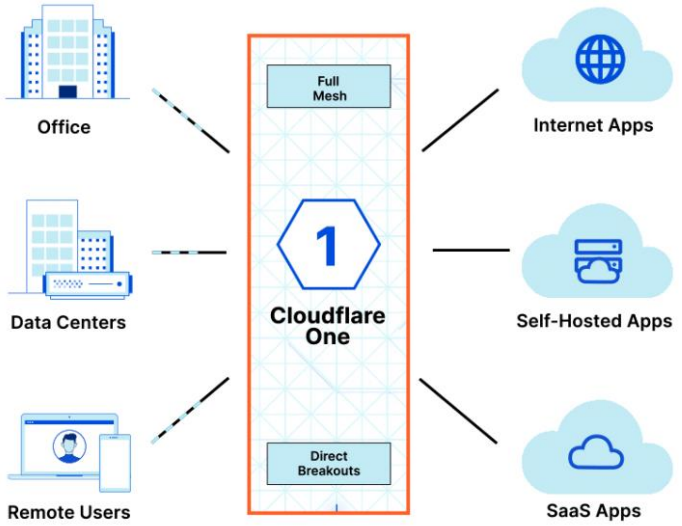
Outside-in

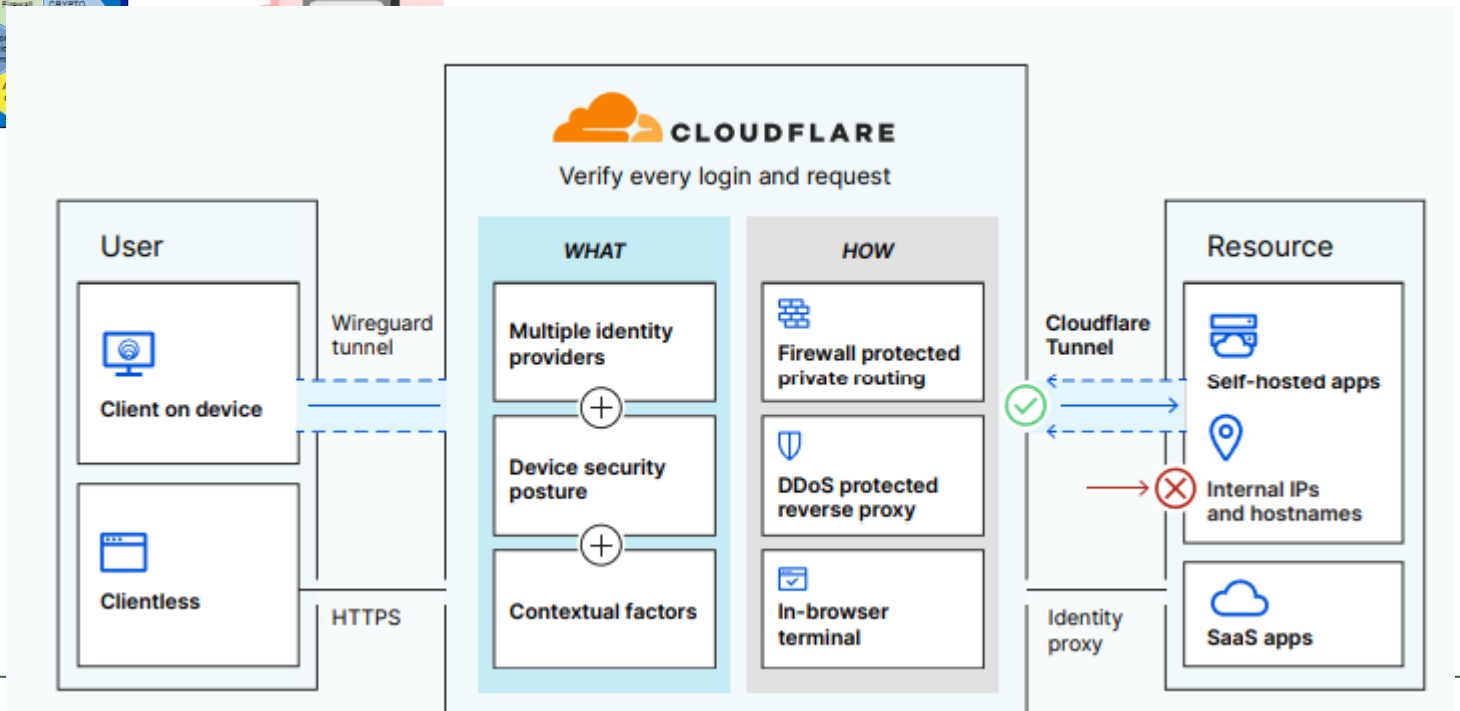
"I'm not ok, and you're not ok –
and we can't trust the network"

New focus on data and services (passwords and acces control / rights management) and segmentation

New world – Zero Tust







Old School to New World in the (Near) Future

Zero Trust

BeyondCorp

Focus areas such as:

- Assume breach
- Identity verification
- Least priviledge
- MFA
- Microsegmentation (identity, services, groups and functions)
- Endpoint security
- Real-time monitoring
- Handling of security incidents

Hardware hacking

Hvad kan man gøre med fysisk adgang til hardware?

(kort introduktion)

Fysisk adgang til hardware

Hardware er selvfølgelig grundlaget for software, algoritmer og kommunikation

Hardware skal sikre, at kun den autentificerede bruger har adgang til processoren

Men:
Hardware design har normalt ikke sikkerhed som et nøgle-designmål

Hardware kan ofte være det svage led i sikre systemer

Fysisk sikkerhed er mange forskellige ting

HOWTO defeat a sliding chain lock with a rubber band:
http://www.youtube.com/watch?v=7INIRLe7x0Y

Locked suitcase:
https://www.youtube.com/watch?v=G5mvvZl6pLI

Opening a computer lock cable:
http://www.youtube.com/watch?v=TPDgX9P8xLQ

Cykellås:
http://www.youtube.com/watch?v=_2vLtpVPqhI

Bypassing security measures

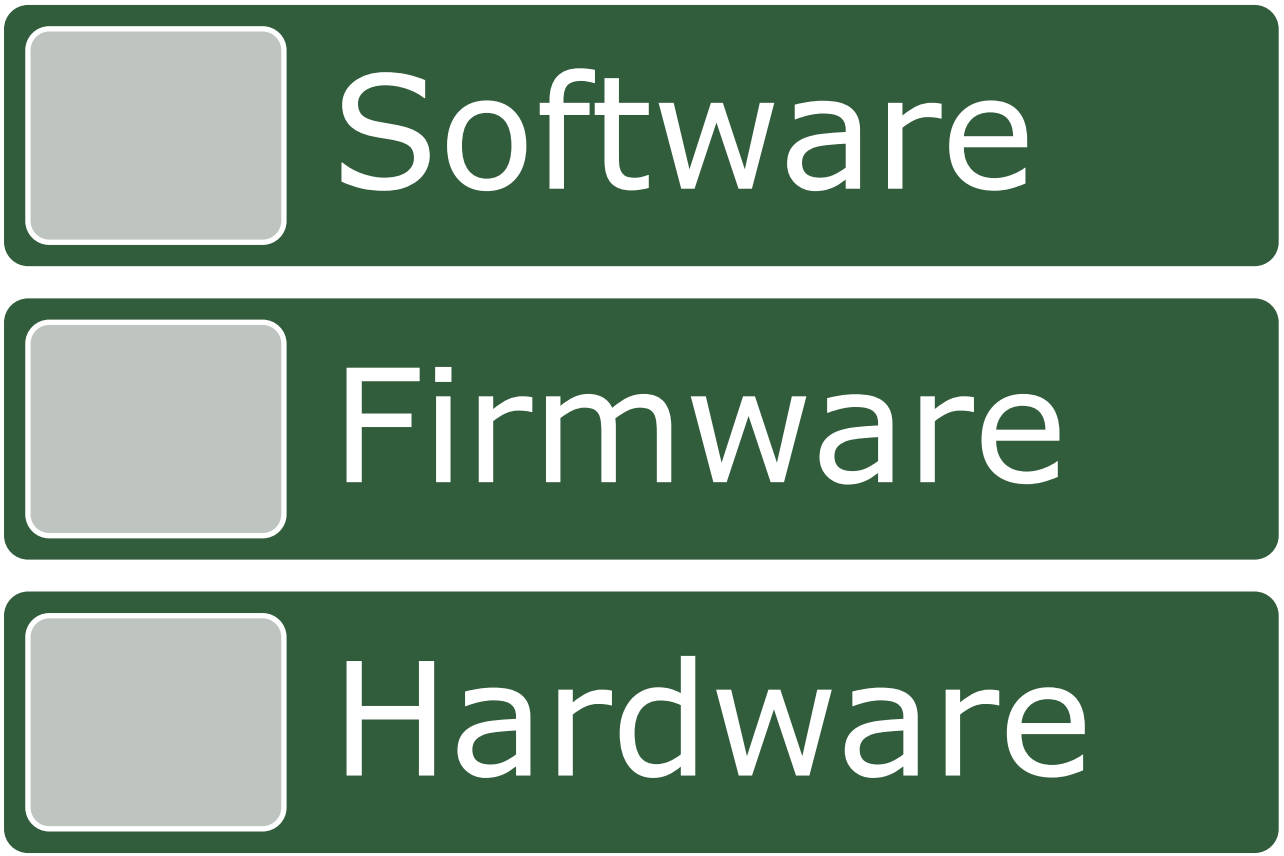
Fysisk sikkerhed er mange forskellige ting

Evil Maid attacks

IOT


Retweeted by the grugq
Matt Haughey @mathowie · 13 hrs
What am I doing? Oh just waiting for my garage door opener to join WiFi so I can get back into my house #2014problems
Verizon
9:51 AM
62%
Places
PLACE
Garage Door Opener
No Response
MyQ Server not responding. Please try again later.
OK

Tre niveauer



Why defend hardware?

Kan enheder klones?
(økonomisk tab pga salg af kopi-enheder, risiko for negative omtale fordi folk tror enhederne er ægte osv)

Kan softwaren stjæles?
Kan hardware design stjæles?
Kan angriber ændre funktionalitet?

Hvor stort budget har angriberen, hvor motiverede er de, kan angriber ødelægge enheden?

Rejsekort – bilnøgler - militære enheder
Supply chain security/verification

People will have physical access to the hardware

Smart cards, phones, cars, RFID, TV etc., etc…

Software

Firmware updates

RAM dump (keys, credit card info etc)

So what can you do to test or assess hardware?

Fysisk adgang til hardware

1. Design walk-through:
High level impression (messy, professional, hidden)

ChipWorks, iFixIt etc. take apart many types of hardware
Can be good starting points, otherwise time for desoldering components - and Google

2. Find interaction points - explore with a multimeter to catalogue hardware interaction points and potential debug interfaces.

Fysisk adgang til hardware

Mass produced hardware needs to be tested prior to deployment.

Interesting or problematic areas of the board have testing points exposed on the outer layers so external testing machines quickly can validate them on the production line.

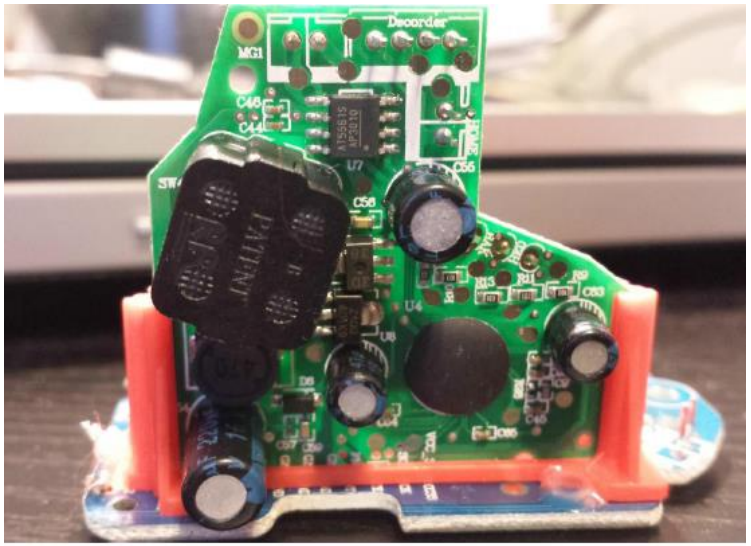
Hardware designers tend to expose debug functionality with these interaction points to allow for firmware and OS flashing post production.

Fysisk adgang til hardware

Tracing all the pins and attempting to recreate the full schematic.
Then acquire spec sheets for every piece of silicon

Start looking for **debug or flashing capabilities**.
The main focus of this part of a hardware analysis is to plan an **attack to grab the resident firmware - or ram**.

Also explore the USB side of the hardware and look at an available driver/os/kernel

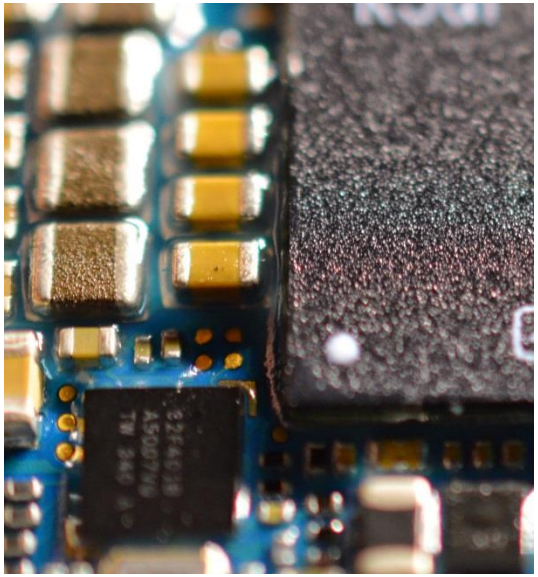


Fysisk adgang til hardware

What we really care about is:

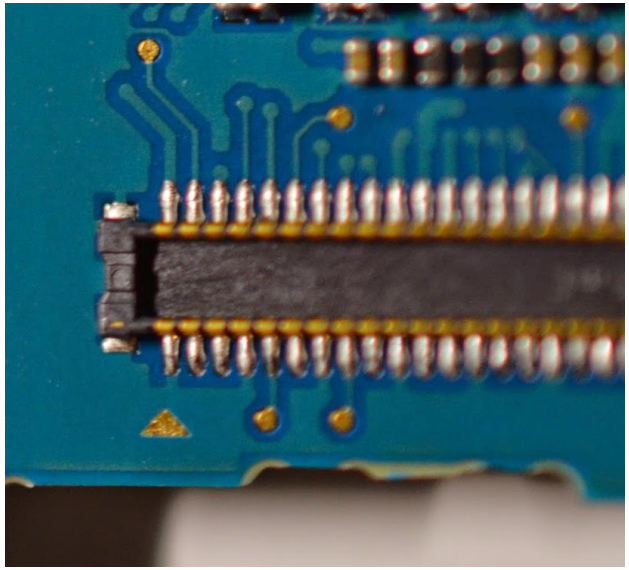
- What components are being used
- How was the device built
  Did the designers leave any debugging mechanisms exposed or active during production
- Are there any weak parts of the design that look easily exploitable

Fysisk adgang til hardware



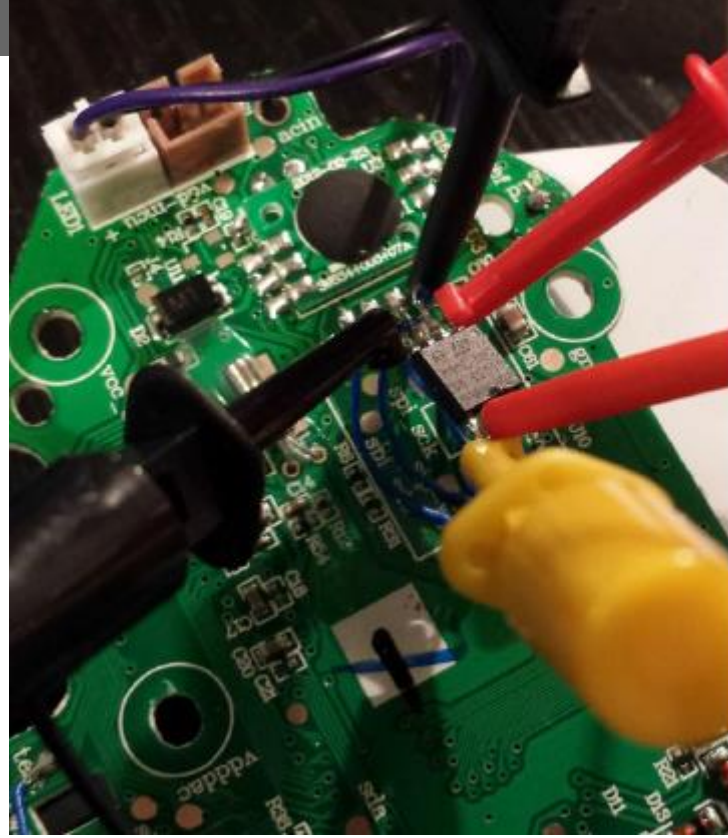
The device must be loaded with software and most vendors protect that functionality with a series of hardware flags controlled by resident voltages. Tracing the pads with a multimeter to see where the missing discrete components would effect, and what circuit they could complete if bridged.

Fysisk adgang til hardware



Ribbon cable seat. The pinouts can be latched with a logic analyzer to watch all the data pass over the cable is possible - much easier than tapping the cables directly.

Fysisk adgang til hardware



Nintendo Wii
Tweezer hack –> private keys

Buffer overflow in save system of Legend of Zelda: Twilight Princess:

Using a modified save file containing a name for Link's horse long enough to cause a buffer overflow pointing to a memory address which contained the loader code.

APP

Side-channel attacks

What else can I do with the device?

Side-channel attacks

Can successfully reveal the secret cryptographic keys stored in secure systems

These attacks include:

- power analysis,
- timing attacks, and
- electromagnetic attacks

Fysisk adgang til hardware

Extracting the Private Key from a TREZOR with a 70 $ Oscilloscope

http://johoe.mooo.com/trezor-power-analysis

Hardware hacking

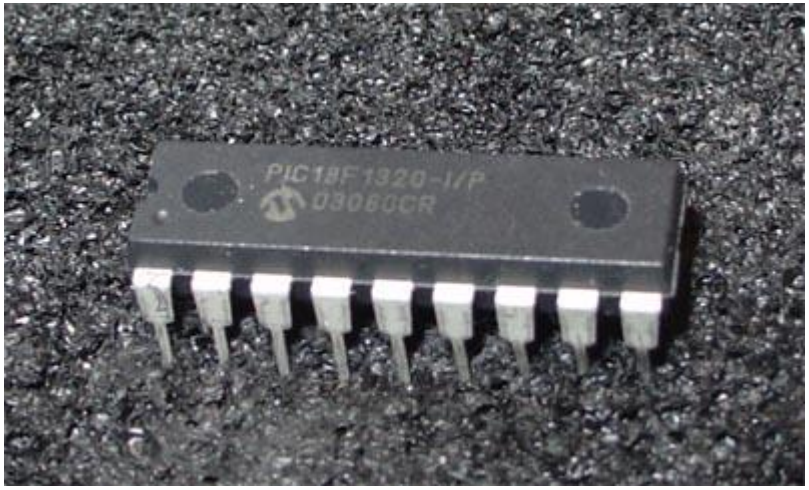
Physically attacks against the chip to extract the key

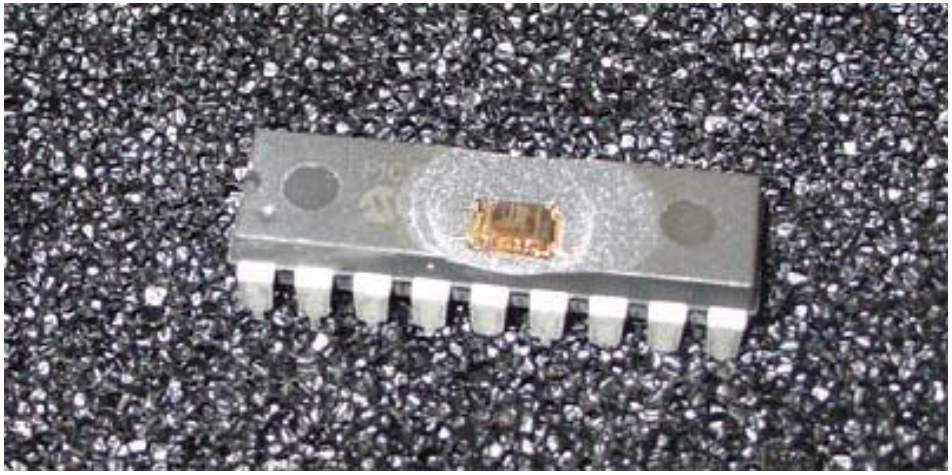
30.000 dollars for "real" microskope, but still not unrealistic

A chip can get cappet for less than 80 dollars on the internet + 600 dollars for an adequate microskope

Decapping chips with acid

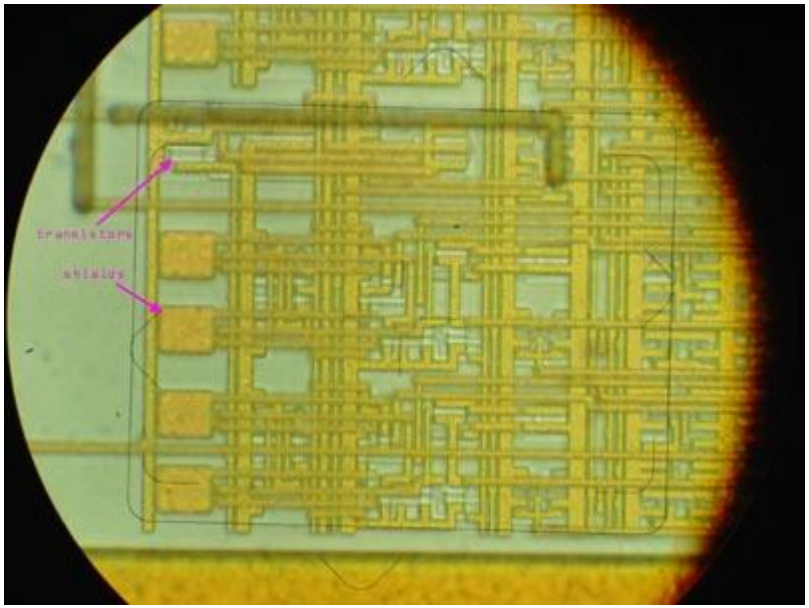
Microskope
Probe when the chip has power

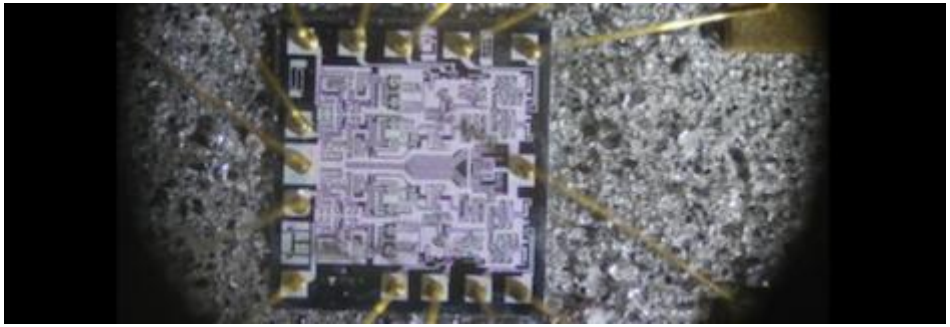




Decapping chips with acid

Microskope
Probe when the chip has power

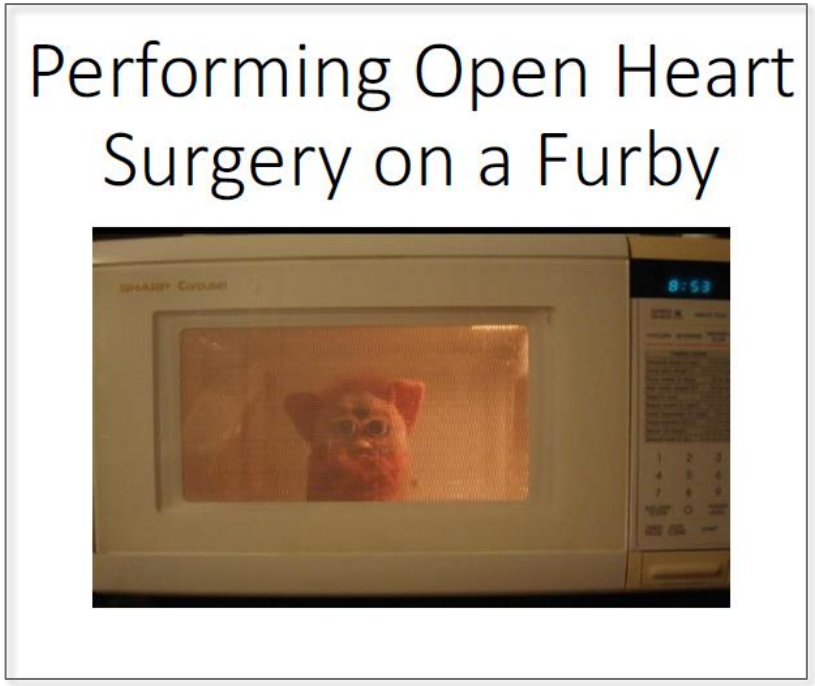




Decapping chips with acid

Microskope
Probe when the chip has power

Hardware hacking – a couple of starting points



http://recon.cx/2014/slides/Performing%20Open%20Heart%20Surgery%20on%20a%20Furby%20Recon%202014.pdf

http://www.siliconpr0n.org/

Lecture plan

Week	Date	Time	Instructor	Topic
36	05 Sep	10-12	TL	Security concepts and principles
	09 Sep	10-12	TL	Cryptographic building blocks
37	12 Sep	10-12	TL	Key establishment and certificate management
	16 Sep	10-12	CJ	User authentication, IAM
38	19 Sep	10-12	CJ	Operating systems security, web, browser and mail security
	23 Sep	10-12	CJ	IT security management and risk assessment
39	26 Sep	10-12	TL	Software security - exploits and privilege escalation
	30 Sep	10-12	TL	Malicious software
40	03 Oct	10-12	CJ	Firewalls and tunnels, security architecture
	07 Oct	**10-12**	**CJ**	**Cloud and IoT security**
41	10 Oct	10-12	TL	Intrusion detection and network attacks
	14 Oct	10-12	TL	Forensics
42				Fall Vacation - No lectures
43	24 Oct	10-12	CJ	Privacy and GDPR
	28 Oct	10-12	CJ	Privacy engineering
44	31 Oct	10-11	Guest	Special topic
		11-12	TL,CJ	Exam Q/A

https://github.com/diku-its/its-e2022/blob/main/lectureplan2022.md

Questions

E-mail security

S/MIME (Secure/Multipurpose Internet Mail Extensions), Pretty Good Privacy (PGP)

- Encrypt and authenticate individual emails using certifcates

DomainKeys Identified Mail (DKIM)

- Authenticates that the email originates from the owner of the domain
- Each email is signed by public key announced in DNS

Sender Policy Framework (SPF)

- Authenticates that a mail claiming to come from a specific domain is submitted by an IP address authorized by that domain's administrators announced in DNS